Вадим Максимович Гудонис, Никита Андреевич Аншаков
Астраханский государственный университет,
ул. Татищева, 20а, г. Астрахань, 414056, Россия
e-mail:gudonis95@gmail.com, ORCID 0000-0002-2392-0331
e-mail:nanshakov@gmail.com, ORCID 0000-0003-4897-2469

БЕЗОПАСНЫЙ ОБМЕН ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ МЕЖДУ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ И ЕГО КЛИЕНТАМИ

DOI: http://dx.doi.org/10.26583/bit.2017.3.03

Аннотация. В статье анализируется взаимодействие удостоверяющих центров и их клиентов. Рассматриваются информационные потоки, возникающие при таком взаимодействии. Далее автор делает вывод о возможности ускорения информационных потоков и упрощения вышеупомянутого взаимодействия путем создания специальной информационной системы. Для данной системы возникает необходимость обеспечить защиту обрабатываемых ей персональных данных. В статье проводится анализ информационной системы с точки зрения нормативно-правовых актов, регламентирующих защиту персональных данных на территории РФ и делается вывод какую степень защищённости персональных данных необходимо обеспечить.

Ключевые слова: электронная подпись, удостоверяющий центр, защита персональных данных, обмен электронными документами.

Для цитирования. **ГУДОНИС, Вадим Максимович; АНШАКОВ, Никита Андреевич.** БЕЗОПАСНЫЙ ОБМЕН ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ МЕЖДУ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ И ЕГО КЛИЕНТАМИ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 30-36, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/261>. Дата доступа: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.03.

Vadim Maksimovich Gudonis, Nikita Andreevich Anshakov
Astrakhan State University, 20a, Tatischev Street, Astrakhan, 414056, Russia
e-mail:gudonis95@gmail.com, ORCID 0000-0002-2392-0331
e-mail:nanshakov@gmail.com, ORCID 0000-0003-4897-2469

Secure exchange of electronic documents between the certifying center and its customers

DOI: http://dx.doi.org/10.26583/bit.2017.3.03

Abstract. The author analyzes the interaction of certifying centers and their clients and the information flows arising from such interaction. Further, he concludes that it is possible to speed up information flows and simplify the above-mentioned interaction by creating a special information system. It is necessary to protect the personal data processed by this system. The author analyzes the information system from the point of view of normative legal acts regulating the personal data protection in the Russian Federation and concludes what degree of protection of personal data is necessary.

Keywords: electronic signature, certification authority, personal data protection, electronic documents exchange.

For citation. **GUDONIS, Vadim Maksimovich; ANSHAKOV, Nikita Andreevich.** Secure exchange of electronic documents between the certifying center and its customers. IT Security, [S.l.], v. 24, n. 3, p. 30-36, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/261>. Date accessed: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.03.

В настоящее время юридически значимый электронный документооборот используется все шире. При этом, для придания электронному документу юридической значимости используется механизм электронной подписи [1].

Главным нормативно-правовом документом, регламентирующим условия использования электронной подписи на территории Российской Федерации, является Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». В нем выделены три разновидности электронной подписи: простая, усиленная неквалифицированная и усиленная квалифицированная. Простая электронная подпись формируется с помощью конфиденциального ключа и содержится в самом электронном документе, тем самым подтверждая сам факт формирования электронной подписи. Усиленная неквалифицированная электронная подпись должна быть сформирована с помощью криптографического средства электронной подписи и ключа электронной подписи, которые обеспечивают возможность ее проверки, в также обнаружение факта изменения электронного документа. Усиленная квалифицированная электронная подпись обязательно используется с сертификатом ключа проверки электронной подписи, созданным только удостоверяющим центром, аккредитованным уполномоченным федеральным органом в отношении удостоверяющих центров. Документ, подписанный действующей электронной подписью, обладает равной с традиционным бумажным документом правомочностью [2].

Для получения электронной подписи гражданину необходимо обратиться в один из аккредитованных удостоверяющих центров, предоставив ряд документально подтвержденных данных, которые перечислены в Федеральном Законе «Об электронной подписи», а также заключить договор на оказание услуг по выпуску электронной подписи. Процессы взаимодействия удостоверяющего центра и его клиентов можно разделить на несколько групп в зависимости от целей клиента:

- получение электронной подписи;
- изменение электронной подписи;
- приостановление действия электронной подписи;
- возобновление действия электронной подписи;
- аннулирование электронной подписи.

Для всех перечисленных групп был проведен анализ информационных потоков взаимодействия удостоверяющего центра и его клиентов. Диаграммы типовых потоков [3-5] данных некоторых из них представлены на рисунках 1 и 2.

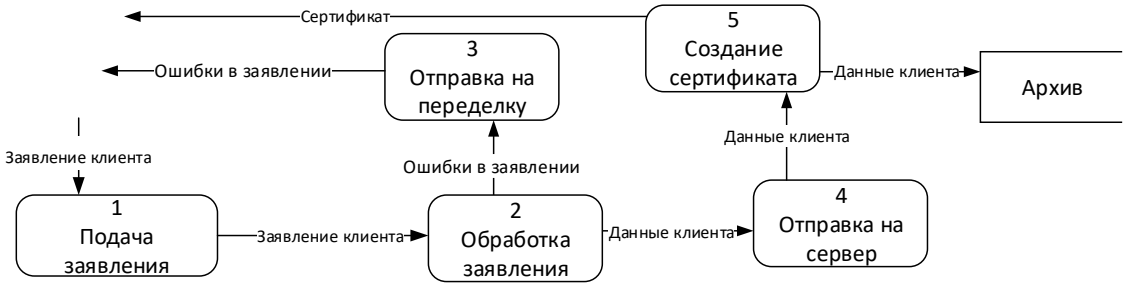

Рисунок 1 - Диаграмма потоков данных при обращении за электронной подписью
(Fig. 1 – Data flow diagram when applying for electronic signature)

Диаграмма потоков данных при обращении за электронной подписью иллюстрирует все случаи, когда необходимо создать или пересоздать измененный сертификат электронной подписи. В таких случаях обработка обращения клиента начинается с проверки его заявления и прилагаемых к нему данных. Если клиент нигде не ошибся, то производится генерация сертификата электронной подписи и отправка данных клиента в

архив. Сгенерированный сертификат ключа проверки электронной подписи выдается клиенту.

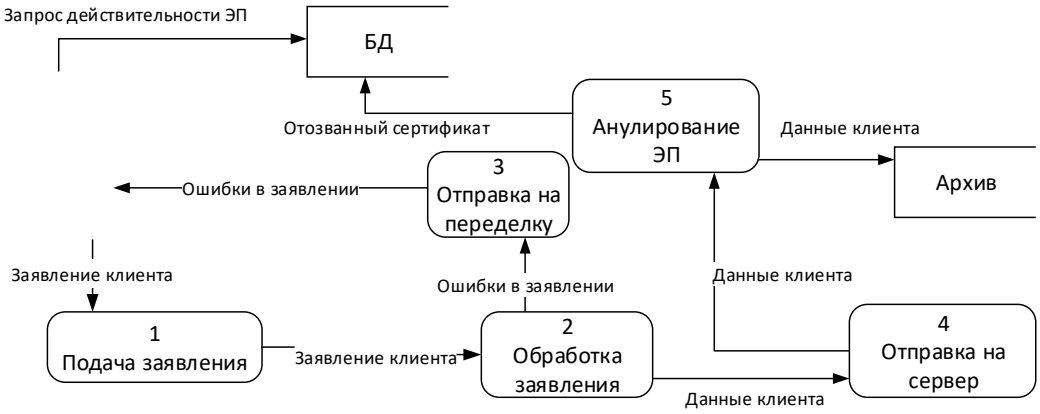

Рисунок 2 - Диаграмма потоков данных при обращении для аннулирования электронной подписи
(Fig. 2 – Data flow diagram when applying for revocation of an electronic signature

Диаграмма потоков данных при обращении для аннулирования электронной подписи иллюстрирует все случаи, когда нужно остановить (на время или навсегда) действие сертификата электронной подписи. Ее отличие от ранее рассмотренной диаграммы обусловлено тем, что отозванный сертификат необходимо поместить в список отозванных сертификатов, находящийся в открытом доступе.

Можно заметить, что обе диаграммы имеют одинаковую часть (см. рисунок 3). Так происходит потому, что при любом взаимодействии с клиентом сотрудникам удостоверяющего центра необходимо проверить его обращение на корректность предоставляемых данных и соблюдение норм оформления обращения.

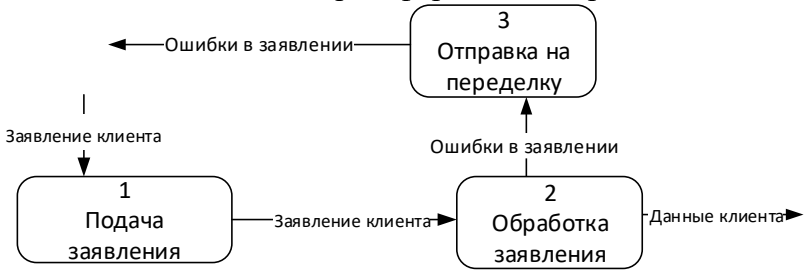

Рисунок 3 - Повторяющаяся часть диаграмм потоков данных
(Fig. 3 – A recurring part of a data flow diagram)

В настоящее время удостоверяющие центры собирают предоставляемую клиентом информации на бумажных носителях. Такой подход долог, трудоемок, и приводит к большому времени ожидания ответной реакции, даже в случае, когда клиент подает все документы правильно заполненными с первого раза. Если же рассматривать намного более часто встречающийся случай, при котором клиент совершает ошибки, то время- и трудозатраты значительно увеличиваются.

Чтобы уменьшить данные недостатки, некоторые удостоверяющие центры предлагают предварительно отправлять им через информационно-телекоммуникационную сеть все необходимые данные, чтобы совместно с клиентом подготовить необходимый набор документов. Сам выпуск происходит при получении подписанных бумажных оригиналов документов.

Такой подход, хоть и значительно ускоряет процесс, но вносит определенный элемент дублирования при оформлении и проверке документов. Максимально избавиться

от этого недостатка можно, если подаваемые клиентом документы в электронном виде будут подписаны электронной подписью, выданной ему ранее. Таким образом, подаваемые документы получат юридическую значимость и пропадет необходимость в их повторной подаче в удостоверяющий центр на бумажных носителях. В данном случае, пакет документов на бумажном носителе необходим только при получении клиентом своей первой электронной подписи.

Для реализации юридически значимого документооборота между удостоверяющими центрами и их клиентами предлагается создать информационную систему, которая принимала бы от пользователя заявление на оказание нужной услуги и все необходимые для этого данные и автоматически генерировала соответствующие документы, позволяя подписывать пакет документов электронной подписью и подавать в электронном виде, а также давая возможность вывода документов на печать.

Очевидно, что в данной системе будет обрабатываться большой объем персональных данных [6] клиентов удостоверяющего центра. В соответствии с действующим законодательством такая информационная система должна быть защищена согласно требованиями, утвержденным Постановлением Правительства РФ от 01.11.2012 № 1119 [7].

Для того чтобы узнать конкретный перечень обязательных (в зависимости от конкретных параметров системы) для реализации мер защиты, рассмотрим классификацию данной информационной системы. Для этого определим категорию обрабатываемых персональных данных, количество субъектов, данные которых будут обрабатываться и тип угроз информационной системы. Также сразу заметим, что обрабатываться будут персональные данные субъектов, не являющихся сотрудниками оператора. Категорию персональных данных определим, как иные персональные данные, так как они не относятся ни к специальным, ни к биометрическим, ни к общедоступным. Рассматриваемый тип угроз – третий. К нему относятся угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. Таким образом согласно Постановлению Правительства РФ от 01.11.2012 № 1119 для рассматриваемой информационной системы будет необходимо обеспечить четвертый или третий уровень защищенности персональных данных, в зависимости от того, обрабатываются персональные данные меньше или больше чем 100 000 субъектов соответственно [8].

В соответствии с Приказом ФСТЭК России от 18.02.2013 г. № 21 информационная система персональных данных четвертого уровня защищённости должна включать в себя перечень мер и механизмов защиты, содержащий 27 наименований, которые перечислены в Приложении к данному Приказу [9].

Информационная система персональных данных [10, 11] третьего уровня защищённости помимо вышеперечисленного должна также включать в себя еще 14 позиций, также перечисленных в Приложении к Приказу.

Согласно Приказу, в информационной системе для обеспечения четвертого уровня защищённости персональных данных также необходимо будет применять:

- средства вычислительной техники не ниже шестого класса;
- системы обнаружения вторжений и средства антивирусной защиты и межсетевые экраны не ниже пятого класса.

Для обеспечения третьего уровня защищённости:

- средства вычислительной техники не ниже пятого класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже четвертого класса;
- межсетевые экраны не ниже третьего класса.

В случае, если информационная система, обеспечивающая электронный документооборот между удостоверяющим центром и его клиентами, является подсистемой государственной информационной системы [12], то она должна соответствовать требованиям Приказа ФСТЭК России от 11.02.2013 г. № 17 [13]. Чтобы узнать конкретный перечень требований нужно определить класс защищенности информационной системы. Он зависит от масштаба информационной системы (федеральный, региональный, объектовый) и уровня значимости, обрабатываемой в ней информации. Последний в свою очередь отражает степень возможного ущерба в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности). Ущерб может быть высоким, средним или низким и в зависимости от его величины информации присваивается уровень значимости от первого (высокий ущерб) до третьего (низкий ущерб).

Для рассматриваемой информационной системы не имеет смысла выносить какие-либо из ее сегментов за пределы объектов удостоверяющего центра, так как хранить и обрабатывать поступающую информацию намного безопасней [14] и дешевле централизовано, поэтому далее будем рассматривать информационную систему объектового масштаб. Вероятный ущерб от нарушений свойств безопасности определяется как низкий, так как удостоверяющий центр даже после нарушения сможет осуществлять свою деятельность. Таким образом информационная система получает третий класс защищенности, то есть для нее должна обеспечиваться нейтрализация угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового [15]. Совокупность мер и средств защиты информации необходимых для этого перечислена в Приложении к Приказу № 17 и эквивалентна мерам, перечисленным в Приложении к Приказу ФСТЭК России от 18.02.2013 г. № 21 и применяемых для об обеспечения третьего уровня защищённости. Требования к средствам вычислительной техники, обнаружения вторжений, антивирусной защиты и межсетевым экранам также совпадают. Соответственно, обеспечиваемый при этом уровень безопасности информационной системы выходит не ниже, чем у системы третьего уровня защищенности по классификации Постановления Правительства РФ от 01.11.2012 № 1119.

Информационная система, обеспечивающая электронный документооборот между удостоверяющим центром и его клиентами, позволит значительно ускорить процесс оказания услуги по выпуску электронной подписи, сократив время на создание и проверку документов. При этом, степень защищенности персональных данных, обрабатываемых в данной информационной системе должна соответствовать третьему классу защищенности согласно Приказа ФСТЭК России от 11.02.2013 г. № 17 или третьему уровню защищенности согласно Приказа ФСТЭК России от 18.02.2013 г. № 21.

СПИСОК ЛИТЕРАТУРЫ

1 Остроушко А.В. К вопросу о правовом регулировании оборота электронной подписи. Правовая информатика. 2013. № 1. С. 51-55.

2 Федеральный Закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3 Кулябов Д.С., Королькова А. В. Введение в формальные методы описания бизнес-процессов: Учебное пособие. – М.: РУДН, 2008. С. 62-66.

4 Аминов Х.И. Моделирование бизнес-процессов: Учебное пособие. – Санкт-Петербург, 2016. С. 31-35.

5 Петеляк В.Е., Новикова Т.Б., Масленникова О.Е., Махмутова М.В., Агдавлетова А.М. Data flow diagramming: особенности построения моделей описания управления потоками данных в организационных системах. Фундаментальные исследования. 2015. № 8-2. С. 323-327.

6 Бойкова О.Ф. Персональные данные: обработка, использование и защита: Методические рекомендации. – Российская государственная библиотека, НИО библиотековедения. Москва, 2013.
7 Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
8 Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. №1119.
9 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
10 Шакалов М.С. Система защиты персональных данных при их обработке в информационной системе персональных данных. Педагогическое образование на Алтае. 2014. № 2. С. 453-454.
11 Меньшикова А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения. Экономика и менеджмент инновационных технологий. 2014. № 11 (38). С. 156-159.
12 Гончаров И.В., Гончаров Н.И., Кирсанов Ю.Г., Паринов П.А., Райков О.В. Проблемы обеспечения безопасности информационных систем персональных данных и государственных информационных систем. ИТ-Стандарт. 2016. Т. 1. № 2-1 (7). С. 46-48.
13 Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
14 Евстратенко Е.С., Селифанов В.В., Старикова А.А. Построение системы защиты информации государственной информационной системы с учетом управления рисками информационной безопасности. Научные исследования: от теории к практике. 2016. № 1 (7). С. 154-157.
15 Мищенко В.И., Шилов А.К. Защита информации в государственных информационных системах. Вестник компьютерных и информационных технологий. 2015. № 3 (129). С. 45-47.

REFERENCES:

[1]Ostroushko A.V. To the question of the legal regulation of the turnover of the electronic signature. Pravovaya informatika. 2013. № 1. P. 51-55. (in Russian).
[2]Federal'nyy Zakon ot 06.04.2011 № 63-FZ «Ob elektronnoy podpisi».
[3]Kulyabov D.S., Korol'kova A. V. Introduction to formal methods of describing business processes: Uchebnoe posobie. – M.: RUDN, 2008. P. 62-66. (in Russian).
[4]Aminov Kh.I. Modeling business processes: Uchebnoe posobie. – Sankt-Peterburg, 2016. P. 31-35. (in Russian).
[5]Petelyak V.E., Novikova T.B., Maslennikova O.E., Makhmutova M.V., Agdavletova A.M. Data flow diagramming: osobennosti postroeniya modeley opisaniya upravleniya potokami dannykh v organizatsionnykh sistemakh. Fundamental'nye issledovaniya. 2015. № 8-2. P. 323-327. (in Russian).
[6]Boykova O.F. Personal data: obrabotka, ispol'zovanie i zashchita: Metodicheskie rekomendatsii. – Rossiyskaya gosudarstvennaya biblioteka, NIO bibliotekovedeniya. Moskva, 2013. (in Russian).
[7]Federal'nyy Zakon ot 27.07.2006 g. № 152-FZ «O personal'nykh dannykh».
[8]Postanovlenie Pravitel'stva Rossiyskoy Federatsii «Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» ot 1 noyabrya 2012 g. №1119.

[9]Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 21 «Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh».
[10] Shakalov M.S. The system of protection of personal data during their processing in personal data information systems. Pedagogicheskoe obrazovanie na Altae. 2014. № 2. P. 453-454. (in Russian).
[11] Men'shikova A.V. Some problems of protection of personal data of the employee, prospects and ways of their solution. Ekonomika i menedzhment innovatsionnykh tekhnologiy. 2014. № 11 (38). P. 156-159. (in Russian).
[12] Goncharov I.V., Goncharov N.I., Kirsanov Yu.G., Parinov P.A., Raykov O.V. The problem of security of personal data information systems and state information systems. IT-Standart. 2016. T. 1. № 2-1 (7). P. 46-48. (in Russian).
[13] Prikaz FSTEK Rossii ot 11 fevralya 2013 g. № 17 «Ob utverzhdenii Trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh».
[14] Evstratenko E.S., Selifanov V.V., Starikova A.A. Building the information security system of the state information system in view of information security risk management. Nauchnye issledovaniya: ot teorii k praktike. 2016. № 1 (7). P. 154-157. (in Russian).
[15] Mishchenko V.I., Shilov A.K. Protection of information in state information systems. Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2015. № 3 (129). P. 45-47. (in Russian).