УДК 35.072

Косогов Дмитрий Олегович, студент Курского филиала Финансового университета при Правительстве РФ, начальник отдела режима секретности и безопасности информации Управления Федерального казначейства по Курской области
e-mail: Vidjit@rambler.ru

ПРАКТИКА ВЗАИМОДЕЙСТВИЯ ТЕРРИТОРИАЛЬНОГО ОРГАНА ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА С ОРГАНИЗАЦИЯМИ – ЗАЯВИТЕЛЯМИ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

Аннотация: в статье приводятся требования по защите информации при осуществлении электронного документооборота, средства, обеспечивающие защищенный обмен документами, перечень документов, связанных с обеспечением безопасности информации при организации обмена электронными документами.
Ключевые слова: электронный документооборот, защита информации, информационная безопасность, средства криптографической защиты информации.

Kosogov Dmitry Olegovich, student of the Kursk branch of Financial University under the Government of the Russian Federation, head of department of the mode of privacy and safety of information of Federal Treasury Department for Kursk region
e-mail: Vidjit@rambler.ru

PRACTICE OF INTERACTION OF TERRITORIAL AUTHORITY OF FEDERAL TREASURY WITH THE ORGANIZATIONS – APPLICANTS CONCERNING SAFETY OF INFORMATION AT IMPLEMENTATION OF EXCHANGE OF ELECTRONIC DOCUMENTS

Summary: requirements for information security at implementation of electronic document flow, the means providing the protected exchange of documents, the list of the documents connected with safety of information at the organization of exchange of electronic documents are provided in article.
Keywords: electronic document flow, information security, information security, means of cryptographic information security.

Территориальный орган Федерального казначейства (далее – ТОФК) в рамках, полученных в территориальном органе Федеральной службы безопасности Российской Федерации лицензий на деятельность, связанную с применением и распространением средств криптографической защиты

информации, несет ответственность за соблюдение организациями – заявителями (далее – Клиенты) требований информационной безопасности, установленных законодательством Российской Федерации [4].

Договором об обмене электронными документами или договором присоединения (соглашение) к Регламенту Удостоверяющего центра Федерального казначейства (далее – Договор) предусмотрена обязанность Клиентов выполнять требования по защите информации, установленные Инструкцией «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 (далее – Инструкция ФАПСИ № 152).

Как показывает практика зачастую Клиенты, подписывая Договор, не считают нужным ознакомиться с содержанием вышеназванной Инструкции ФАПСИ № 152. В это время для них главное – как можно быстрее перейти на обмен электронными документами, о значимости защиты информации при этом никто не задумывается. И если мы не разъясним Клиенту, чем обусловлены требования по защите информации при осуществлении обмена электронными документами, в чем заключаются эти требования, если не обяжем Клиента обеспечить выполнение требований, то они, как правило, останутся невыполненными.

Требования по защите информации при осуществлении обмена электронными документами, содержащими конфиденциальную информацию (сведения, связанные с финансированием Клиентов, являются конфиденциальной информацией), обусловлены следующими обстоятельствами:

1) обмен электронными документами осуществляется по незащищенным каналам связи. В связи с этим возможен несанкционированный доступ к информации, в результате чего возможно ознакомление с информацией посторонних лиц, внесение каких-либо изменений в передаваемые электронные документы, т.е. подделка документа;

2) в случае невыполнения Клиентами требований по защите информации, применяемые при обмене электронными документами ключи электронных подписей и аутентификации, а также программные средства криптографической защиты информации могут стать доступны посторонним лицам. Если этим воспользуется злоумышленник, подготовленный в техническом отношении, тщательно проработавший схему своих корыстных действий, это может иметь для Клиента серьезные негативные последствия [1].

С учетом вышеизложенных обстоятельств безопасность информации при осуществлении обмена электронными документами обеспечивается применением средств криптографической защиты информации и организационными мерами.

Средства криптографической защиты информации обеспечивают защиту электронных документов от несанкционированного доступа при их передаче по незащищенным каналам связи, в том числе:

– средство электронной подписи обеспечивает защиту электронных документов от их подделки;

– средство аутентификации обеспечивает защиту электронных документов от ознакомления с содержащейся в них информацией.

Организационные меры должны исключать неконтролируемый доступ к средствам криптографической защиты информации и ключевой информации и включают в себя:

– опечатывание средств вычислительной техники, на которые установлены программные средства криптографической защиты информации;

– хранение носителей ключевой информации в надежно запираемых и опечатываемых хранилищах;

– осуществление контроля целостности печатей на средствах вычислительной техники, на которых установлены средства криптографической защиты информации, и хранилищах с носителями ключевой информации;

– своевременным обнаружением фактов несанкционированного доступа к средствам криптографической защиты информации и носителям ключевой информации;

– своевременными и правильными действиями должностных лиц Клиента в случае компрометации ключей электронных подписей и аутентификации [2].

В основу обеспечения выполнения Клиентами требований по защите информации при осуществлении обмена электронными документами положено максимальное повышение роли и ответственности работника Клиента, назначенного администратором автоматизированного рабочего места обмена электронными документами (далее – администратор АРМ), который в соответствии с Договором отвечает, в частности, за контроль мероприятий по защите информации и взаимодействие с Организатором по вопросам обеспечения безопасности информации [3].

С этой целью наряду с обучением администраторов АРМ Клиентов правилам применения средств криптографической защиты информации, также проводится инструктивное занятие, в ходе которого доводятся и поясняются разработанные ТОФК нормативные, технические и вспомогательные документы, в том числе обязанности администратора АРМ, методические рекомендации по выполнению требований Инструкции ФАПСИ № 152, порядок уведомления о компрометации ключа электронной подписи, аутентификации и другие.

При проведении инструктивного занятия администраторам АРМ разъясняется, о необходимости ведения документации, связанной с обеспечением безопасности информации при организации обмена электронными документами. К такой документации относится:

– дело с нормативными, техническими и вспомогательными документами, связанными с организацией обмена электронными документами;

– дело с перепиской с ТОФК по вопросам организации обмена электронными документами;

– дело с документами постоянного хранения, связанными с организацией обмена электронными документами;

– журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним;

– журнал поэкземплярного учета ключевых документов;

– журнал учета обучения пользователей средств криптографической защиты информации.

Обучению и прохождению инструктивного занятия подлежит каждый вновь назначенный Клиентом администратор АРМ. При этом проверяется наличие у Клиента необходимых документов, связанных с обеспечением безопасности информации при организации обмена электронными документами, и их передача вновь назначенному администратору АРМ.

Таким образом, вышеизложенная практика взаимодействия ТОФК с организациями – участниками бюджетного процесса обеспечивает выполнение требований руководящих и нормативных документов по защите информации, и также необходимый уровень безопасности информации при осуществлении обмена электронными документами.

Список литературы:

1. Инструкция «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 // СПС КонсультантПлюс.

2. Письмо Федерального казначейства от 19 июля 2013 г. N 42-7.4-05/10.1-433 «О Примерном договоре об обмене электронными документами» // СПС КонсультантПлюс.

3. Косогов Д.О. Безопасность информации при электронном документообороте // XIII Международная студенческая научная конференция «Мировой опыт и экономика регионов России». – Курск, 2015. – С. 141-143.

Официальный сайт Федерального казначейства – URL: www.roskazna.ru

4. Официальный сайт УФК по Курской области – URL: www.kursk.roskazna.ru.