Наталия ЖОВНИЦКАЯ, *редактор направления «Бухгалтерский учет и налогообложение»*

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ: ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

Как обеспечивает орган Казначейства защиту личных ключей с электронной подписью от несанкционированного доступа к ним во время обслуживания распорядителей (получателей) средств, которые осуществляют обмен документами в электронном виде через программно-целевой комплекс «Клиент Казначейства – Казначейство», выясним в этой консультации.

Нормативные требования

Прежде всего напомним, что **дистанционное казначейское обслуживание** – это такой электронный документооборот, в котором не принимают участие бумажные носители, что существенно экономит как финансовые, так и трудовые расходы.

Вместе с тем **электронный документооборот,** или **оборот электронных документов** – это совокупность процессов создания, обработки, отправления, передачи, получения, хранения, использования и уничтожения электронных документов, которые выполняются с применением проверки целостности и в случае необходимости с подтверждением факта получения таких документов.

Осуществление обмена электронными документами между органом Казначейства и распорядителями и получателями бюджетных средств (далее – бюджетные учреждения) происходит путем дистанционного обслуживания клиентов с использованием программно-технического комплекса «Клиент Казначейства – Казначейство», что предусмотрено распоряжением КМУ от 15.11.17 г. № 816-р «Некоторые вопросы дистанционного обслуживания распорядителей (получателей) бюджетных средств».

Для осуществления обмена документами в электронном виде бюджетные учреждения применяют **электронные документы** и **квалифицированную электронную подпись** (далее – КЭП). Основные организационно-правовые принципы электронного документооборота и использования электронных документов устанавливает Закон от 22.05.03 г. № 851-IV «Об электронных документах и электронном документообороте» (далее – Закон № 851).

Согласно ст. 5 Закона № 851 **электронный документ** – это документ, в котором информация зафиксирована в виде электронных данных, которые содержат обязательные реквизиты документа.

Электронный документ может быть создан, передан, сохранен, а также преобразован электронны-

***силу**, как этот же документ на бумаге.*

Если электронный документ нужно отправить нескольким адресатам или сохранить на нескольких электронных носителях, то информация каждого из электронных экземпляров считается оригиналом электронного документа.

Казначейства – Казначейство» согласно законодательству.

Перечень электронных документов, которыми бюджетные учреждения имеют право обмениваться с органами Казначейства путем использования системы дистанционного обслуживания (далее – СДО), приведем в таблице.

№ п/п	Наименование документа
1	**2**
1	Сеть распорядителей и получателей бюджетных средств (реестры изменений в нее)
2	Распределения показателей сводных смет, сводных планов ассигнований общего фонда бюджета (за исключением предоставления кредитов из бюджета), сводных планов специального фонда бюджета (за исключением собственных поступлений бюджетных учреждений и соответствующих расходов), свод показателей специального фонда (реестры изменений в них)
3	Распределения открытых ассигнований и распоряжения на выделение ассигнований местного бюджета
4	Реестры бюджетных обязательств, реестры бюджетных финансовых обязательств и подтверждающие документы
5	Платежное поручение на перечисление средств со счетов с именами получателей, которые имеют право подписывать электронные документы
6	Выписки со счетов с именами получателей, которые имеют право подписывать электронные документы, протоколы расхождений данных сети распорядителей и получателей бюджетных средств и Единого реестра распорядителей бюджетных средств и получателей бюджетных средств, извлечения из Единого реестра распорядителей бюджетных средств и получателей бюджетных средств
7	Выписки со счетов по поступлениям
8	Смета, план ассигнований (за исключением предоставления кредитов из бюджета) общего фонда бюджета, план использования бюджетных средств, помесячный план использования бюджетных средств, план предоставления кредитов из общего фонда бюджета, план специального фонда государственного бюджета (за исключением собственных поступлений бюджетных учреждений и соответствующих расходов), свод показателей специального фонда сметы и справки об изменениях в них

Количество подписей, которые налагаются на отдельный тип документа, определяется учреждением самостоятельно согласно нормативным документам, но на электронный документ, сформированный учреждением, должно налагаться не менее чем две КЭП.

Требования к защите информации

Вся информация, которой обмениваются бюджетные учреждения и органы Казначейства, должна быть надежно защищена и недоступна для посторонних лиц. Система защиты информации должна обеспечивать целостность, конфиденциальность и аутентичность электронных документов. Это предусмотрено п. 2 Положения о технической защите информации в Украине, утвержденного Указом Президента от 27.09.99 г. № 1229/99.

Для достижения необходимого уровня защищенности информационного обмена бюджетные учреждения должны осуществить программно-технические и организационные мероприятия, такие как:

- установка защищенной сессии путем использования комплекса криптографической защиты информации, который имеет подтвержденное соответствие;
- обеспечение трудоспособности СДО сетью передачи данных, подключенной к защищенному узлу Интернет-доступа;
- назначение на основании приказа учреждения лица, ответственного за наложение ЭЦП в СДО и эксплуатацию клиентской части программного

учреждением и органом Казначейства, регламента работы Казначейства как квалифицированного предоставителя электронных доверительных услуг, а также с соответствующими инструкциями по эксплуатации.

Личные ключи ответственных лиц и печати должны быть записаны на защищенные носители личных ключей. Носители личных ключей должны находиться в опечатанном сейфе, с обеспечением доступа к ним только ответственным лицам, которые назначены по приказу учреждения и которые имеют право наложения ЭЦП СДО.

Заметим, что бюджетные учреждения обязаны использовать только защищенные носители ключевой информации, и именно это обеспечивает защиту личных ключей ЭЦП от несанкционированного доступа к ним. Также этого требует политика безопасности программно-технических комплексов «Клиент Казначейства – Казначейство» и АС «Э-Отчетность».

Кроме того, на веб-портале Казначейства изложен перечень защищенных носителей основной информации (токенов), которые могут быть использованы для работы в программно-технических комплексах «Клиент Казначейства – Казначейство» и АС «Е-Отчетность».

И напоследок заметим, что в случае нарушения требований относительно обеспечения защиты информации **виновные должностные лица несут ответственность** согласно действующему законодательству.