Ассоциация Электронных Торговых Площадок

«Удостоверяющие центры: пределы доверия. Практика авторизации удостоверяющих центров при федеральных операторах электронных торговых площадок и АЭТП»

Удостоверяющие центры. Что они удостоверяют?

РИТЬ - Засвидетельствовать правильность, подлинность, точность чего-нибудь. Удостоверить чью-нибудь подпись. 2. Убедить в истинности чего-нибудь...*Толковый словарь Ушакова*

Удостоверить — заверить, засвидетельствовать, подтвердить, убедить, уверить, освидетельствовать, скрепить, констатировать *(Словарь русских синонимов)*

Удостоверяющий центр

УЦ — это организация, которая не только в определенной степени **заменяет нотариальные конторы** для **однократного заверения** документов, собственноручной подписи, а **вручает пользователю в руки инструмент для многократного** юридически значимого технического **заверения** электронных документов **в течение года или другого периода**.

Результат доверия:

Совершение пользователем
(владельцем сертификата ЭП)
серии юридически значимых действий,
в т.ч. сделок на колоссальные суммы.

Цена обманутого доверия:

Признание подписанных ЭП документов,
сделок на колоссальные суммы
юридически ничтожными.

Тот, кто удостоверяет, должен располагать кредитом доверия не столько со стороны государственных органов, но в большей мере - организаторов и участников системы электронного юридически значимого документооборота (СЭДО)

Кредит доверия к УЦ складывается из:

гарантий регуляторов и контролирующих инстанций (лицензии, свидетельства об аккредитации, свидетельства о вхождении в сеть доверия и т.п.)

результатов постоянного мониторинга со стороны контролирующих органов

публичной репутации УЦ на рынке СЭДО (PR, публикации в СМИ, обсуждения на форумах, возможных конфликтных событий, проблем у клиентов, компрометации ЭП)

ФАКТОРЫ СНИЖЕНИЯ ДОВЕРИЯ к УЦ и СЭДО:

➢**невысокая цена гарантий контролирующих инстанций** в случае неквалифицированной проверки УЦ, отсутствия постоянного контроля и мониторинга за деятельностью УЦ;

➢**отсутствие механизмов ответственности института контролеров** в виде компенсации пострадавшей стороне;

➢**недоверие участников СЭДО к перспективам получения возмещения пострадавшей стороне от страховых компаний** в случае мошенничества или грубых нарушений со стороны УЦ;

➢**неквалифицированная работа персонала УЦ**, склонность к упрощенчеству, нарушению нормативных требований, **стремление владельца УЦ извлечь больше выгоды** путем снижения затрат на соблюдение установленных требований.

➢Общепринятое недоверие к контрагенту: **подозрения в недобросовестности, мошенничестве, причастности к криминальному сообществу**.

Самое страшное – это утрата общественного доверия к институту УЦ и электронному юридически значимому ЭДО в результате крупной аферы

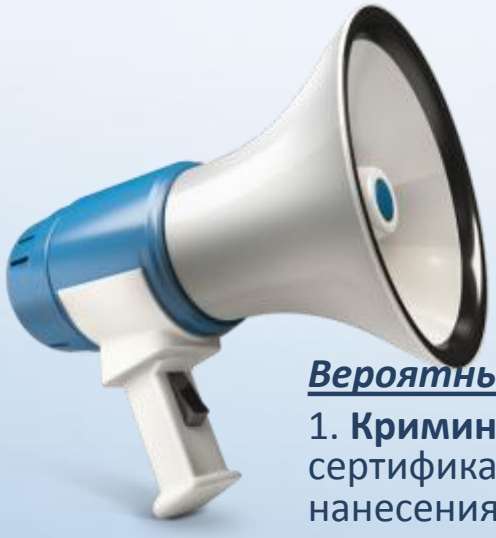
Устремления криминального сообщества к получению фиктивных сертификатов электронной подписи

Методы достижения цели:

- предоставление в УЦ подложных документов для выпуска «левого» сертификата ЭП (на не существующего пользователя, вымышленную организацию или реальную, но к которой будущий владелец ЭП отношения не имеет);
- привлечение для подачи документов в УЦ и получения ключа ЭП «доверенных лиц», используемых «втёмную»;
- вовлечение персонала УЦ в противоправные действия по выпуску нелегитимного сертификата;
- создание (или приобретение) собственного УЦ, готового в нужный момент «выстрелить» очередью фиктивных сертификатов.

В России зафиксирован ряд фактов выпуска фиктивных сертификатов ЭП. О количестве невыявленных «затаившихся» левых сертификатов остается лишь догадываться. Это вирус, проникший в систему доверия.

Методика проверки УЦ должна исходить из угроз!



Методика проверки УЦ и контроля за их деятельностью должна иметь ясно сформулированную **цель: убедиться в готовности УЦ отразить угрозы**. Проверяющая и проверяемая стороны должны иметь четкое понимание **комплексной модели наиболее вероятных угроз УЦ и участникам системы ЭДО,** доверившимся сертификатам, проверяемого УЦ, а не модели абстрактных «угроз информационной безопасности» безотносительно пострадавшей стороны.

Вероятные источники угроз УЦ и участникам СЭДО:

1. **Криминальное сообщество, мошенники**. Результат – выпуск недостоверных сертификатов ЭП, их использование для совершения корыстных преступлений, нанесения ущерба государству и бизнесу.
2. **Неквалифицированный персонал УЦ**. Результат – неработоспособность сертификатов, сбои в функционировании УЦ, несвоевременность публикации СОС, «зависание» пользователей в системе ЭДО.
3. **Бестолковые или «хитромудрые» пользователи**. Попытки сыграть на недочетах УЦ, признать совершенные операции недействительными.
4. **Лицензирующие органы**, добросовестно осуществившие контроль. Результат – приостановка лицензии УЦ, «зависание» всех его пользователей в СЭДО.

Факторы, способствующие реализации угроз выпуска фиктивного сертификата ЭП

1. Нормативная допустимость подачи заявления в УЦ и получения сертификата по доверенности от пользователя.

2. Отсутствие нормативно закрепленной обязанности УЦ приступить к выпуску сертификата только при личной явке и идентификации заявителя. Как результат - массовый выпуск сертификатов по копиям документов, присланных факсом или по эл.почте.

3. Сомнительный статус Приказа ФАПСИ от 13.06.2001 г. №152 (морально устарел, не зарегистрирован в Минюсте, нормы не соответствуют реалиям). По факту: пересылка криптоключей всеми видами почты, передача через проводников поездов и водителей автобусов…

«СИТО КОНТРОЛЯ» за УЦ

со стороны государственных органов:

- ФНС (на стадии регистрации) ;
- ФСБ (при выдаче лицензии на деятельность в области криптографии) ;
- ФНС, ПФР, Росстат, Фонд социального страхования, Росреестр, Росалкогольрегулирование, Федеральная служба по тарифам, Таможенная служба и др. – при заключении договоров о вхождении в доверенные операторы, ФСТЭК (при получении лицензии на ТЗИ) ;
- ЭТП (центры авторизации) – для авторизации на федеральных электронных торговых площадках);
- другие организаторы СЭДО;
- Прочие контролирующие ведомства МВД (контрафакт), МЧС (пожарная охрана), СЭС и др.

Что в действительности проверяется?

- Уставные, регистрационные документы,
- законность использования помещений, аппаратуры, программных средств,
- документы о наличии в штате организации 2-3 сотрудников, отвечающих требованиям по стажу и образованию,
- наличие в УЦ стандартного пакета внутренних инструкций по ИБ,
- наличие договора страхования на 1,5 млн.руб., стоимость чистых активов (Минкомсвязи), банковская гарантия на 1 млн. руб. (ЭТП).

7. Для получения лицензии соискатель лицензии представляет (направляет) в лицензирующий орган заявление о предоставлении лицензии и документы (копии документов), указанные в пунктах 1, 3 и 4 части 3 статьи 13 Федерального закона "О лицензировании отдельных видов деятельности", а также следующие копии документов и сведения:

а) копии правоустанавливающих документов на помещения, здания, сооружения и иные объекты по месту осуществления лицензируемой деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

б) копии внутренних распорядительных документов, подтверждающих наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, определенных настоящим Положением, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";

в) копии документов, подтверждающих нахождение в штате соискателя лицензии на основной работе сотрудников, определенных подпунктом "д" пункта 6 настоящего Положения;

г) копии документов государственного образца (дипломы, аттестаты, свидетельства) об образовании, о переподготовке, повышении квалификации по направлению "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей сотрудников, определенных подпунктом "д" пункта 6 настоящего Положения;

д) копии трудовых книжек сотрудников, определенных подпунктом "д" пункта 6 настоящего Положения;

е) копии должностных инструкций сотрудников, определенных подпунктом "д" пункта 6 настоящего Положения;

ж) копии документов, подтверждающих наличие у соискателя лицензии приборов и оборудования, прошедших поверку и калибровку в соответствии с Федеральным законом "Об обеспечении единства измерений", принадлежащих ему на праве собственности или ином законном основании и необходимых для выполнения работ и оказания услуг, указанных в пунктах 1 - 11, 16 - 19 перечня;

з) сведения о документах, подтверждающих право собственности или иное законное основание на владение и использование помещений, зданий, сооружений и иных объектов по месту осуществления лицензируемой деятельности, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

и) сведения о документе, подтверждающем наличие условий для соблюдения конфиденциальности информации, необходимых для выполнения работ и оказания услуг, определенных настоящим Положением, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации";

к) сведения о документе, подтверждающем наличие допуска к выполнению работ и оказанию услуг, связанных с использованием сведений, составляющих государственную тайну (при выполнении работ и оказании услуг, указанных в пунктах 1, 4 - 6, 16 и 19 перечня).

(Постановление Правительства РФ от 16 апреля 2012 г. N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"

Приложение № 1

УТВЕРЖДЕНО

приказом Министерства связи и массовых коммуникаций

Российской Федерации

от _23.11.2011_ № _320

Правила аккредитации удостоверяющих центров

7. К заявлению прилагаются следующие документы (в том числе необходимые для изготовления квалифицированного сертификата ключа проверки электронной подписи (далее – квалифицированный сертификат), созданного с использованием средств головного УЦ):

1) документ, подтверждающий наличие финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи, выданном таким УЦ, или информации, содержащейся в реестре сертификатов, который ведет такой УЦ, в сумме не менее чем полтора миллиона рублей. Таким документом может являться:

договор страхования ответственности;

банковская гарантия;

договор поручительства.

В случае предоставления банковской гарантии в качестве документа, подтверждающего наличие финансового обеспечения ответственности, заявитель указывает номер лицензии на осуществление банковской деятельности кредитной организации, предоставившей банковскую гарантию.

В случае предоставления договора страхования ответственности в качестве документа, подтверждающего наличие финансового обеспечения ответственности, уполномоченный орган дополнительно проверяет наличие указанной в договоре страхования организации в Едином государственном реестре субъектов страхового дела;

2) актуальная выписка из бухгалтерского баланса, подтверждающая, что стоимость чистых активов УЦ составляет не менее чем один миллион рублей;

3) документы, выдаваемые федеральным органом исполнительной власти в области обеспечения безопасности, подтверждающие соответствие используемых УЦ средств электронной подписи и средств УЦ, требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

4) документы, подтверждающие право собственности УЦ (право использования программы для ЭВМ) либо иное законное основание использования им средств электронной подписи и средств УЦ, указанных в подпункте 3 настоящего пункта;

5) документы, подтверждающие наличие в штате УЦ не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, имеющих высшее профессиональное образование в области информационных технологий или информационной безопасности либо высшее или среднее профессиональное образование с последующим прохождением переподготовки или повышения квалификации по вопросам использования электронной подписи:

копии трудовых договоров (с приложением утвержденных должностных регламентов);

копии документов о высшем профессиональном образовании в области информационных технологий или информационной безопасности (диплом установленного государственного образца) или копии документов о прохождении переподготовки или повышения квалификации по вопросам использования электронной подписи (свидетельства установленного образца);

6) учредительные документы УЦ, либо их надлежащим образом заверенные копии;

7) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);

8) доверенность или иной документ, подтверждающий право уполномоченного лица УЦ, направившего указанные документы, действовать от имени УЦ.

Получение документов, указанных в настоящем пункте и находящихся в распоряжении органов, предоставляющих государственные услуги, органов, предоставляющих муниципальные услуги, иных государственных органов, органов местного самоуправления либо подведомственных государственным органам или органам местного самоуправления организаций, участвующих в предоставлении государственных услуг, осуществляется, в том числе в электронной форме с использованием единой системы межведомственного электронного взаимодействия и подключаемых к ней региональных систем межведомственного электронного взаимодействия по межведомственному запросу уполномоченного органа.

Документы, указанные в настоящем пункте, могут быть представлены УЦ самостоятельно.

8. Дополнительно УЦ, претендующий на получение аккредитации, может представить документы, подтверждающие: наличие необходимых для осуществления деятельности УЦ лицензий в соответствии с требованиями законодательства РФ; внесение УЦ в реестр операторов, осуществляющих обработку персональных данных; наличие Порядка реализации функций удостоверяющего центра, осуществления прав и исполнения обязанностей удостоверяющего центра, соответствующего требованиям законодательства РФ в сфере использования электронной подписи; соответствие требованиям по безопасности информации на объекте информатизации или копия заключения о соответствии требованиям по безопасности информации, выданных ФСТЭК России и ФСБ России в пределах их полномочий.

ПРИКАЗ
от 20 апреля 2012 г. N ММВ-7-6/253@

ОБ УТВЕРЖДЕНИИ ВРЕМЕННОГО ПОЛОЖЕНИЯ О СЕТИ ДОВЕРЕННЫХ ОПЕРАТОРОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ВРЕМЕННОГО ПОЛОЖЕНИЯ О ПОРЯДКЕ ПРИСОЕДИНЕНИЯ К СЕТИ ДОВЕРЕННЫХ ОПЕРАТОРОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

II. Порядок проведения процедуры присоединения к Сети доверенных ОЭД

3.2.2. К заявлению на присоединение к Сети доверенных ОЭД прилагаются следующие документы:

- нотариально заверенная копия учредительных документов;
- нотариально заверенная копия свидетельства о государственной регистрации организации в качестве юридического лица;
- нотариально заверенная копия лицензии ФСБ России на право предоставления услуг в области шифрования информации, не содержащей сведений, составляющих государственную тайну;
- нотариально заверенная копия лицензии ФСБ России на право осуществления деятельности по распространению шифровальных средств;
- нотариально заверенная копия лицензии ФСБ России на право осуществления деятельности по техническому обслуживанию шифровальных средств;
- нотариально заверенная копия лицензии Федеральной службы по техническому и экспортному контролю Российской Федерации на техническую защиту информации;
- нотариально заверенная копия лицензии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на предоставление телематических услуг связи;
- описание к программным средствам оператора электронного документооборота и пользовательская документация к программным средствам, реализующим требования Порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи, утвержденного приказом Минфина России от 25.04.2011 N 50н;
- документы, подтверждающие наличие программно-аппаратных средств для выполнения функций ОЭД, и факт размещения этих средств на территории Российской Федерации;
- перечень средств электронной подписи, применяемых для реализации функций Операторов электронного документа;
- документ, в котором соискатель подтверждает намерения выполнять требования данного Положения и Временного положения о Сети доверенных операторов электронного документооборота.

Документы соискателя должны быть подписаны, а копии, кроме нотариально заверенных, должны быть заверены полномочным лицом соискателя.

Что не изучается государственными контролерами при проверке УЦ:

- **история и обстоятельства образования УЦ, реальность его существования** (если без выездных проверок), наличие признаков «УЦ-однодневки». Т.е. никто не задается вопросом – а не тот ли это УЦ, который изначально предназначен для использования в противоправных целях?
- **квалификация персонала, проверяющего сведения, вносимые в сертификат ключа ЭП**: способность оценить явную подделку, обнаружить признаки недостоверности или юридической незначимости документов (например, просроченный паспорт или доверенность), увидеть и оценить возможные ограничения полномочий получателя сертификата ЭП (например, срок полномочий назначенного директора истекает через несколько дней после выпуска сертификата) и т.п.
- **Не декларативная, а реальная технология работы УЦ**, (кто именно из персонала участвует в генерации закрытого сертификата, кто этих людей заменяет в период отпусков и т.п., кем и как эти ключи передаются пользователю, кто и как обучает пользователя использованию СКЗИ и инструктирует на случай компрометации ключей, как хранится документация, послужившая основанием для выпуска сертификата ЭП и т.п.). Как производится идентификация пользователей?.
- **Осмысленно не проверяется** на соответствие требованиям ФЗ №63 **Регламент УЦ**, хотя он запрашивается всеми проверяющими (кроме ФСБ).
- **Минкомсвязью не проверяется наличие лицензий** у аккредитуемых УЦ на деятельность в области криптографии
- **принципиально не изучается сеть обособленных подразделений УЦ**,
- не изучаются **лицензионные полномочия как самих УЦ, так и их партнерских точек** выдачи сертификатов!
- не изучаются **факты привлечения аккредитованными УЦ к изготовлению криптоключей, распространению и обслуживанию СКЗИ нелицензированных партнеров**, ИП и просто физлиц.

Из перечня разрешенных видов деятельности согласно Постановлению Правительства №313:

- п.28. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

КОПИЯ

УФСБ России по Ростовской области

ЛИЦЕНЗИЯ

ЛСЗ № 0000122 * Рег. № 3317 от «29» июля 2013 г.

На осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств информационных систем и телекоммуникационных систем

Общему с ограниченной ответственностью

УДОСТОВЕРЯЮЩИЙ ЦЕНТР «

(ООО УЦ «

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1136165002192

Идентификационный номер налогоплательщика 6165180356

А нужно ли уметь читать лицензию?

УСЛОВИЯ ДЕЙСТВИЯ ЛИЦЕНЗИИ:

1. Действие лицензии распространяется на:

– шифрование информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц;

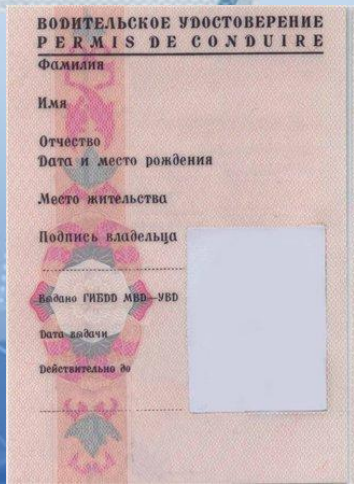
– обеспечение пользователей системы электронного документооборота ключевой информацией (включая ее формирование и распределение) независимо от вида носителя ключевой информации, предназначенной для защиты информации, не содержащей сведений, составляющих государственную тайну.

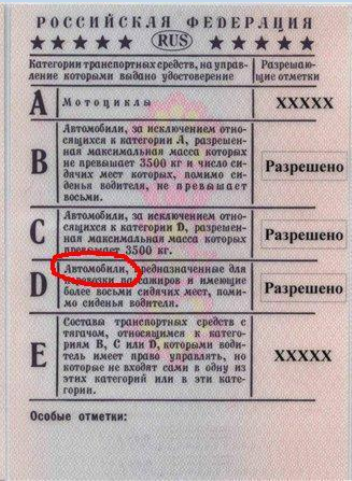
2. Соблюдение лицензионных требований и условий, определенных для разрешенного лицензией вида деятельности.

3. Лицензия дает право Обществу с ограниченной ответственностью «[redacted]» осуществлять предоставление услуг в области шифрования информации в его системах электронного документооборота.

4. Предоставление прав на занятие указанным в лицензии видом деятельности филиалам Общества с ограниченной ответственностью «[redacted]» осуществляется в соответствии с отдельным решением Лицензирующего органа.

5. Лицензия не освобождает Общество с ограниченной ответственностью «[redacted]» от необходимости получения отдельных лицензий на право предоставления услуг в области шифрования информации в других системах.





Приоритетные цели при проверке УЦ в рамках авторизации на федеральных ЭТП:

Определение уровня подготовленности персонала УЦ к

- ***предотвращению действий мошенников,***
- *плановым и неплановым проверкам,* ***недопущению*** *санкций (****приостановки действия лицензий****) со стороны лицензирующего органа.*

Выявление предпосылок и минимизация рисков:

- **признания** сертификатов ЭП и подписанных такими ЭП документов **юридически ничтожными** вследствие неквалифицированной проверки персоналом УЦ первичного пакета заявительских документов от будущего пользователя, **нарушения условий информационной безопасности** при формировании закрытого сертификата и **при выдаче** криптоключа пользователю.
- необеспечения **надежности функционирования УЦ** (дублирование электропитания, адресов публикации СОС, автоматизация процесса, резервирование данных);
- **технических дефектов** при выпуске сертификатов ЭП,
- **неадекватности персонала, в т.ч. руководства УЦ**

Первоапрельские наивные вопросы:

- Понимают ли регуляторы, что их **непродуманные формулировки и необоснованное повышение требований** к УЦ лихорадит эту сферу и влечет огромные затраты, **приводит к удорожанию услуг для пользователей, в т.ч. государственных учреждений??**
- **Чем обоснованы** новые требования **по квалификации и стажу персонала**?
- Как собираются исправлять формулировку «… сведения о документах **государственного образца** (дипломы, аттестаты, свидетельства) об образовании, о переподготовке, повышении квалификации по направлению "Информационная безопасность» …
- **Отвечают ли сами проверяющие этим требованиям**?
- Знают ли они, что **государственные УЦ, как правило, не располагают таким персоналом**?
- Не потому ли так разнятся формулировки по персоналу в №63-ФЗ и ПП-313?
- **Чем не устраивали 4 вида** деятельности в сфере криптографии, зачем их стало 28?
- Кто-то может наизусть произнести название постановления №313? Сколько слов в названии этого Постановления?
- не является ли **нарушением антимонопольного законодательства** формулировка п.8 ст.16 №63-ФЗ « На государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, осуществляющие функции удостоверяющих центров, не распространяются требования, установленные пунктами 1 и 2 части 3 настоящей статьи».
-Предлагаемое изменение 63-ФЗ в части повышения размера страхового обеспечения УЦ вне зависимости от объема выпуска сертификатов до 50 млн.руб. обосновано какими-то расчетами? Отталкивается от прецедентов? Почему не 3, не 20, не 150?
- Не пора ли исключить возможность получения криптоключа в УЦ по доверенности?

«Не нужно кошмарить бизнес!» {УЦ} (В.В.Путин)

Требования регуляторов не состыкованы между собой и не согласовывались с основными операторами СЭДО.

Лицензирующие, аккредитующие гос.органы не доверяют друг другу, формально проверяют одно и то же (наличие документов, но не суть), ответственности перед УЦ и участниками СЭДО не несут.

Требования регуляторов зачастую носят формальный и неоправданно затратный характер, не исходят из реальной модели угроз, толкают бизнес на обман. Ведут к удорожанию услуг УЦ.

Вмененные затраты УЦ (размер страхового обеспечения, банковских гарантий, чистых активов) не обоснован расчетами.

Вместо помощи УЦ, формирования разумного прозрачного пространства – равнодушие, неоперативность реагирования и дополнительное обременение (СМЭВ и т.п.)

Проверяй и доверяй!

Адекватные УЦ нуждаются и сами заинтересованы в периодической квалифицированной, качественной, доброжелательной проверке, методологической помощи, внешнем мониторинге и аудите, постоянной информационной и технической поддержке.

Сообщество УЦ заинтересовано в стабильности, равных правилах для всех, прозрачной системе требований и оценок их работы, недопущении скандалов на рынке УЦ.

Государство и регуляторы не хотят ЧП, скандальных событий, связанных с реализацией установок Президента РФ в направлении «электронного правительства», СЭДО.

Ассоциация Электронных Торговых Площадок в лице Центра авторизации УЦ готова делиться наработками по проверке и мониторингу УЦ со всеми заинтересованными государственными и коммерческими структурами.

Вместе мы наведем порядок в системах ЭДО, обеспечим их процветание и спокойствие участников ЭДО за собственное благополучие.

Спасибо за внимание!

Вопросы???

Заместитель Генерального директора,
руководитель Комиссии по авторизации УЦ
Панов Валентин Николаевич
panov@aetp.ru