Об утверждении критериев оценки степени рисков в области информатизации, связи, за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи

Утративший силу

Совместный приказ Министра по инвестициям и развитию Республики Казахстан от 29 июня 2015 года № 735 и и.о. Министра национальной экономики Республики Казахстан от 30 июня 2015 года № 494. Зарегистрирован в Министерстве юстиции Республики Казахстан 14 августа 2015 года № 11891. Утратил силу совместным приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 30 декабря 2015 года № 1275 и и.о. Министра национальной экономики Республики Казахстан от 31 декабря 2015 года № 841

Сноска. Утратил силу совместным приказом и.о. Министра по инвестициям и развитию РК от 30.12.2015 № 1275 и и.о. Министра национальной экономики РК от 31.12.2015 № 841 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с подпунктом 2) пункта 1 статьи 11 и пунктом 3 статьи 13 Закона Республики Казахстан от 6 января 2011 года «О государственном контроле и надзоре в Республике Казахстан» **ПРИКАЗЫВАЕМ**:

1. Утвердить:

1) Критерии оценки степени рисков в области информатизации согласно приложению 1 к настоящему совместному приказу;

2) Критерии оценки степени рисков в области связи согласно приложению 2 к настоящему совместному приказу;

3) Критерии оценки степени рисков за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи согласно приложению 3 к настоящему совместному приказу.

2. Признать утратившим силу совместный приказ Министра связи и информации Республики Казахстан от 31 августа 2011 года № 263 и Министра экономического развития и торговли Республики Казахстан от 16 сентября 2011 года № 305 «Об утверждении критериев оценки степени риска в сфере частного предпринимательства в области информатизации, связи, за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи» (зарегистрированный в Реестре государственной регистрации нормативных правовых актов за № 7262, опубликованный в газете «Казахстанская правда» 12 ноября 2011 года № 361-362

(26752-26753).

3. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Казангап Т.Б) обеспечить:

1) государственную регистрацию настоящего совместного приказа в Министерстве юстиции Республики Казахстан;

2) в течение десяти календарных дней после государственной регистрации настоящего совместного приказа в Министерстве юстиции Республики Казахстан направление его копии на официальное опубликование в периодических печатных изданиях и информационно-правовой системе «Әділет»;

3) размещение настоящего совместного приказа на интернет-ресурсе Министерства по инвестициям и развитию Республики Казахстан и на интранет-портале государственных органов;

4) в течение десяти рабочих дней после государственной регистрации настоящего совместного приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства по инвестициям и развитию Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2) и 3) пункта 3 настоящего совместного приказа.

4. Контроль за исполнением настоящего совместного приказа возложить на курирующего вице-министра по инвестициям и развитию Республики Казахстан.

5. Настоящий совместный приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр по инвестициям и развитию Республики Казахстан
_____А. Исекешев

Исполняющий обязанности Министра национальной экономики Республики Казахстан
_____ М. Кусаинов

«СОГЛАСОВАН»
Председатель Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан
_____ С. Айтпаева
13 июля 2015 год

Приложение 1
к совместному приказу
Министра по инвестициям и развитию
Республики Казахстан
от 29 июня 2015 года № 735
и исполняющего обязанности

Министра национальной экономики Республики Казахстан
от 30 июня 2015 года № 494

Критерии оценки степени риска в области информатизации

1. Общие положения

1. Настоящие Критерии оценки степени риска в области информатизации (далее - Критерии) разработаны в соответствии с Законом Республики Казахстан от 6 января 2011 года «О государственном контроле и надзоре в Республике Казахстан» для отнесения проверяемых субъектов к степеням риска и отбора проверяемых субъектов при проведении выборочных проверок.

2. В настоящих Критериях используются следующие понятия:

1) проверяемые субъекты в области информатизации (далее – проверяемые субъекты) – владельцы электронных информационных ресурсов, информационных систем;

2) риск - вероятность причинения вреда в результате деятельности проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства с учетом степени тяжести его последствий;

3) объективные критерии оценки степени риска (далее – объективные критерии) – критерии оценки степени риска, используемые для отбора проверяемых субъектов (объектов) в зависимости от степени риска в определенной сфере деятельности и не зависящие непосредственно от отдельного субъекта (объекта);

4) субъективные критерии оценки степени риска (далее – субъективные критерии) – критерии оценки степени риска, используемые для отбора проверяемых субъектов (объектов) в зависимости от результатов деятельности конкретного проверяемого субъекта (объекта);

5) система оценки рисков – комплекс мероприятий, проводимый органом контроля и надзора, с целью назначения проверок.

3. Критерии оценки степени риска для выборочных проверок формируются посредством объективных и субъективных критериев.

2. Объективные критерии

4. Определение риска в области информатизации осуществляется в зависимости от вероятности причинения вреда в результате деятельности

проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства деятельностью проверяемых субъектов, связанную с бесконтрольным использованием контрольно-кассовых машин и информационных систем, интегрируемых с государственными информационными системами, которое может привести к утечке информации государственных органов путем несанкционированного доступа к информационным системам, а также к отсутствию фискализации поступающих платежей на контрольно-кассовые машины являющиеся компьютерной системой .

5. В области информатизации к высокой степени риска относятся проверяемые субъекты аттестованные на соответствие требованиям информационной безопасности негосударственные информационные системы, интегрируемые с государственными информационными системами.

6. К проверяемым субъектам, не отнесенным, к высокой степени риска относятся проверяемые субъекты, получившие заключения для включения в государственный реестр контрольно-кассовых машин контрольно-кассовые машины, являющиеся компьютерной системой.

7. В отношении проверяемых субъектов, отнесенных к высокой степени риска проводятся выборочные проверки.

3. Субъективные критерии

8. Определение субъективных критериев осуществляется с применением следующих этапов:

1) формирование базы данных и сбор информации;

2) анализ информации и оценка рисков.

9. Формирование базы данных и сбор информации необходимы для выявления проверяемых субъектов, нарушающих законодательство Республики Казахстан в области информатизации.

Анализ информации и оценка субъективных критериев позволит сконцентрировать проверки в отношении проверяемого субъекта с наибольшим потенциальным риском. При этом, при анализе и оценке не применяются данные субъективных критериев, ранее учтенных и использованных в отношении конкретного проверяемого субъекта.

Для оценки степени рисков по субъективным критериям используются следующие источники информации:

1) результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) проверяемых субъектов. При этом, степень тяжести

нарушений (грубое, значительное, незначительное) устанавливается в случае несоблюдения требований законодательства Республики Казахстан в области информатизации, отраженных в проверочных листах;

2) наличие и количество подтвержденных жалоб и обращений на проверяемых субъектов, поступивших от физических или юридических лиц, государственных органов.

10. Оценка степени риска проверяемых субъектов и отнесение их к высокой или проверяемых субъектов, не отнесенных к высокой степени риска по субъективным критериям осуществляется по следующим показателям:

1) по информационному источнику «результаты предыдущих проверок (выборочных, внеплановых и иных форм контроля)» субъективные критерии определяются согласно приложению 1 к настоящим Критериям;

2) по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов» субъективные критерии определяются согласно приложению 2 к настоящим Критериям.

11. Определение степени риска по каждому информационному источнику определяется следующим образом.

Одно невыполненное требование грубой степени приравнивается к показателю 100 и это является основанием для проведения проверки в выборочном порядке.

В случае если нарушение требований грубой степени не выявлено, то для определения показателя степени риска рассчитывается суммарный показатель требований значительной и незначительной степени.

При определении показателя нарушений значительной степени применяется коэффициент 0,7 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_з = (\Sigma P_2 \times 100 / \Sigma P_1) \times 0,7$$

где:

$\Sigma P_з$ – показатель нарушений значительной степени;

ΣP_1 – общее количество индикаторов значительной степени, предъявленных к проверке (анализу) проверяемому субъекту (объекту);

ΣP_2 - количество нарушенных требований значительной степени.

При определении показателя нарушений незначительной степени применяется коэффициент 0,3 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_н = (\Sigma P_2 \times 100 / \Sigma P_1) \times 0,3$$

где:

$\sum P_н$ – показатель нарушений незначительной степени;

$\sum P_1$ – общее количество индикаторов незначительной степени, предъявленных к проверке (анализу) проверяемому субъекту (объекту);

$\sum P_2$ - количество нарушенных требований незначительной степени.

Общий показатель степени риска ($\sum P$) рассчитывается по шкале от 0 до 100 и определяется путем суммирования показателей по следующей формуле:

$$\sum P = \sum P_з + \sum P_н$$

где:

$\sum P$ - общий показатель степени риска;

$\sum P_з$ - показатель нарушений значительной степени;

$\sum P_н$ - показатель нарушений незначительной степени.

По показателям степени риска проверяемый субъект (объект) относится:

1) к высокой степени риска – при показателе степени риска от 60 до 100 и в отношении него проводится выборочная проверка;

2) не отнесенной к высокой степени риска – при показателе степени риска от 0 до 60 и в отношении него не проводится выборочная проверка.

4. Заключительные положения

12. Кратность проведения выборочной проверки составляет 1 раз в год и определяется по результатам проводимого анализа и оценки получаемых сведений по субъективным критериям.

13. Выборочные проверки проводятся на основании списков выборочных проверок, формируемых на полугодие по результатам проводимого анализа и оценки, которые направляются в уполномоченный орган по правовой статистике и специальным учетам в срок не позднее, чем за пятнадцать календарных дней до начала соответствующего отчетного периода.

14. Списки выборочных проверок составляются с учетом:

1) приоритетности проверяемых субъектов (объектов) с наибольшим показателем степени риска по субъективным критериям;

2) нагрузки на должностных лиц, осуществляющих проверки, государственного органа.

Приложение 1
к Критериям оценки степени риска в области информатизации

Субъективные критерии по информационному источнику «результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля)»

№	Критерии	Степень нарушени
Результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) (степень тяж устанавливается при несоблюдении нижеперечисленных требований)		
1.	отсутствие изменений условий функциональности, аппаратно-программного комплекса и информационных технологии, информационных систем	грубая
2.	соответствие общей структуры требованиям политики безопасности и размещения компонентов в структуре	незначительная
3.	соответствие конфигурации компонентов, являющихся составляющими информационных систем	незначительная
4.	наличие утвержденной функциональной схемы (план) взаимодействия компонентов информационных систем, а также интегрируемых компонентов информационных систем (физическая и логическая структура информационных систем, пояснительная записка к функциональной схеме)	значительная
5.	наличие организационных мер информационной безопасности эксплуатируемой информационной системы	значительная
6.	наличие Правил паспортизации средств вычислительной техники и использования информационных ресурсов	незначительная
7.	наличие Инструкции о порядке действий пользователей во внештатных (кризисных) ситуациях.	незначительная
8.	наличие Инструкции пользователя по эксплуатации компьютерного оборудования и программного обеспечения	незначительная
9.	наличие Инструкции по организации антивирусной защиты.	значительная
10.	наличие Инструкции о резервном копировании информации.	значительная
11.	наличие Инструкции по закреплению функций и полномочий администратора сервера.	значительная
12.	наличие Правил доступа пользователей и администраторов в серверные помещения.	значительная
13.	наличие Правил регистрации пользователей в корпоративной информационной сети.	значительная
14.	наличие Памятки для работы системных администраторов.	значительная
15.	наличие Памятки пользователю средств вычислительной техники.	значительная
16.	наличие Инструкции по использованию электронной почты и служб Интернет на рабочих станциях.	значительная
17.	наличие лицензий на используемое программное обеспечение и сертификатов соответствия на компьютерное, телекоммуникационное оборудование, терминалы оплаты услуг, торговые автоматы, пос-терминалы и иное оборудование, применяемое в информационном процессе фискального режима компьютерной системы.	грубая
18.	наличие сертификатов соответствия требованиям информационной безопасности технических и программных средств фискального режима, фискальной памяти, входящих в состав компьютерной системы и участвующих в информационном процессе (СТ РК ГОСТ	грубая

	Р ИСО/МЭК 15408-2006 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»).	
19.	соответствие системы безопасности компьютерной системы требованиям к серверному помещению и помещению ограниченного доступа	незначительная
20.	наличие лицензионного или свободно распространяемого антивирусного программного обеспечения с актуальной базой сигнатур на персональных компьютерах пользователей компьютерной системы	незначительная
21.	наличие защищенного канала передачи данных между территориально разделенными подразделениями организации с шифрованием трафика с помощью аппаратных граничных маршрутизаторов.	незначительная
22.	наличие системы обнаружения (предотвращения) атак из сети Интернет посредством межсетевого экрана	значительная
23.	наличие систем идентификации и аутентификации пользователя	значительная
24.	наличие аппаратного сетевого анализатора трафика по идентификатору управления доступом к носителю сетевых карт основного и резервного серверного оборудования компьютерной системы, используемых в фискальном режиме	значительная
25.	наличие системы резервного копирования компьютерной системы	значительная
26.	наличие службы информационной безопасности	значительная
27.	наличие ответственных лиц по компьютерной системе	незначительная
28.	наличие политики информационной безопасности (нормы и практические приемы, регулирующие управление, защиту и распределение информации ограниченного доступа)	грубая
29.	наличие политики формирования и использования паролей	грубая
30.	наличие политики резервного копирования (архивирования)	грубая
31.	наличие документации с описанием процедур по ограничению доступа и обязанностей пользователей, администраторов безопасности, системных администраторов	значительная
32.	наличие сертификата средств криптографической защиты информации согласно СТ РК 1073-2007 «Средства криптографический защиты информации. Общие технические требования» и в зависимости от криптографической стойкости, должны соответствовать уровням безопасности согласно СТ РК 1073-2007	грубая
33.	отсутствие уязвимостей, выявленных при инструментальном обследовании	значительная
34.	наличие фиксирования всех операций компьютерной системы без возможности их дальнейшей корректировки, связанных с торговыми операциями, оказанием услуг посредством наличных денег, а также при формировании фискальных отчетов. Выходные формы фискальных отчетов компьютерной системы заверяются электронной цифровой подписью объекта проверки	значительная
35.	корректная работа функционирующей компьютерной системы, в части функции формирования и проверки электронной цифровой подписи	значительная
36.	наличие акта о соответствии компьютерной системы техническим требованиям для включения в Государственный реестр контрольно-кассовых машин	значительная

Приложение 2
к Критериям оценки степени
риска в области информатизации

Субъективные критерии по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые

субъекты, поступивших от физических или юридических лиц, государственных органов»

№	Критерии	Степень нарушени
1.	наличие одной подтвержденной жалобы или обращения в области информатизации	незначительное
2.	наличие двух или более подтвержденных жалоб или обращений в области информатизации	значительное

Приложение 2
к совместному приказу
Министра по инвестициям и развитию
Республики Казахстан
от 29 июня 2015 года № 735
и исполняющего обязанности
Министра национальной экономики
Республики Казахстан
от 30 июня 2015 года № 494

Критерии оценки степени риска в области связи

1. Общие положения

1. Настоящие Критерии оценки степени риска в области связи (далее - Критерии) разработаны в соответствии с Законом Республики Казахстан от 6 января 2011 года «О государственном контроле и надзоре в Республике Казахстан» для отнесения проверяемых субъектов к степеням риска и отбора проверяемых субъектов при проведении выборочных проверок.

2. В настоящих Критериях используются следующие понятия:

1) операторы связи - физическое или юридическое лицо, оказывающее услуги связи;

2) проверяемые субъекты в области связи (далее – проверяемые субъекты) – операторы связи, владельцы ведомственных и корпоративных сетей телекоммуникаций, отдельного коммутационного оборудования, подключаемого к сети телекоммуникаций общего пользования, владельцы радиоэлектронных средств, являющиеся пользователями радиочастотным спектром;

3) риск - вероятность причинения вреда в результате деятельности проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства с учетом степени тяжести его последствий;

4) объективные критерии оценки степени риска (далее – объективные

критерии) – критерии оценки степени риска, используемые для отбора проверяемых субъектов (объектов) в зависимости от степени риска в определенной сфере деятельности и не зависящие непосредственно от отдельного субъекта (объекта);

5) субъективные критерии оценки степени риска (далее – субъективные критерии) – критерии оценки степени риска, используемые для отбора проверяемых субъектов (объектов) в зависимости от результатов деятельности конкретного проверяемого субъекта (объекта);

6) система оценки рисков – комплекс мероприятий, проводимый органом контроля и надзора, с целью назначения проверок.

3. Критерии оценки степени риска для выборочных проверок формируются посредством объективных и субъективных критериев.

2. Объективные критерии

4. Определение риска в области связи осуществляется в зависимости от вероятности причинения вреда в результате деятельности проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства деятельностью проверяемых субъектов, связанную с:

бесконтрольным использованием платного ограниченного ресурса радиочастотного спектра, которое может привести к возникновению радиопомех и невозможности использования его законными владельцами, а также вредным электромагнитным излучениям;

эксплуатацией оборудования на сетях телекоммуникаций без технических средств проведения специальных оперативно-розыскных мероприятий, которая может привести к невозможности проведения органами оперативно-розыскной деятельности необходимых мероприятий;

нарушением порядка пропуска трафика, которое может привести к невозможности приостановления деятельности любых сетей и средств связи (за исключением правительственной связи) в случае наступления чрезвычайной ситуации социального, природного и техногенного характера.

5. В области связи к высокой степени риска относятся проверяемые субъекты, оказывающие не лицензируемые виды услуги связи, а также владельцы ведомственных и корпоративных сетей телекоммуникаций, отдельного коммутационного оборудования, подключаемого к сети телекоммуникаций общего пользования, владельцы радиоэлектронных средств, являющиеся пользователями радиочастотным спектром.

6. К проверяемым субъектам, не отнесенным, к высокой степени риска

относятся проверяемые субъекты, получившие лицензии на предоставление следующих услуг в области связи: междугородная телефонная связь, международная телефонная связь, сотовая связь (с указанием наименования стандарта), спутниковая подвижная связь.

7. В отношении проверяемых субъектов, отнесенных к высокой степени риска проводятся выборочные проверки.

3. Субъективные критерии

8. Определение субъективных критериев осуществляется с применением следующих этапов:

1) формирование базы данных и сбор информации;

2) анализ информации и оценка рисков.

9. Формирование базы данных и сбор информации необходимы для выявления проверяемых субъектов, нарушающих законодательство Республики Казахстан в области связи.

Анализ информации и оценка субъективных критериев концентрирует проверки в отношении проверяемого субъекта с наибольшим потенциальным риском. При этом, при анализе и оценке не применяются данные субъективных критериев, ранее учтенных и использованных в отношении конкретного проверяемого субъекта.

Для оценки степени рисков по субъективным критериям используются следующие источники информации:

1) результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) проверяемых субъектов. При этом, степень тяжести нарушений (грубое, значительное, незначительное) устанавливается в случае несоблюдения требований законодательства Республики Казахстан в области связи, отраженных в проверочных листах;

2) результаты мониторинга радиочастотного спектра, радиоэлектронных средств и (или) высокочастотных устройств, качества предоставляемых услуг связи;

3) наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов.

10. Оценка степени риска проверяемых субъектов и отнесение их к высокой группе риска и группе риска не отнесенных к высокой степени по субъективным критериям осуществляется по следующим показателям:

1) по информационному источнику «результаты предыдущих проверок (выборочных, внеплановых)» субъективные критерии определяются согласно

приложению 1 к настоящим Критериям;

2) по информационному источнику «результаты мониторинга радиочастотного спектра, радиоэлектронных средств и (или) высокочастотных устройств, качества предоставляемых услуг связи» субъективные критерии определяются согласно приложению 2 к настоящим Критериям;

3) по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов» субъективные критерии определяются согласно приложению 3 к настоящим Критериям.

11. Определение степени риска по каждому информационному источнику определяется следующим образом.

Одно невыполненное требование грубой степени приравнивается к показателю 100 и это является основанием для проведения проверки в выборочном порядке.

В случае если нарушение требований грубой степени не выявлено, то для определения показателя степени риска рассчитывается суммарный показатель требований значительной и незначительной степени.

При определении показателя нарушений значительной степени применяется коэффициент 0,7 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_з = (\Sigma P_2 \times 100/\Sigma P_1) \times 0,7$$

где:

$\Sigma P_з$ – показатель нарушений значительной степени;

ΣP_1 – общее количество индикаторов значительной степени, предъявленных к проверке (анализу) проверяемому субъекту;

ΣP_2 - количество нарушенных требований значительной степени.

При определении показателя нарушений незначительной степени применяется коэффициент 0,3 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_н = (\Sigma P_2 \times 100/\Sigma P_1) \times 0,3$$

где:

$\Sigma P_н$ – показатель нарушений незначительной степени;

ΣP_1 – общее количество индикаторов незначительной степени, предъявленных к проверке (анализу) проверяемому субъекту;

ΣP_2 - количество нарушенных требований незначительной степени.

Общий показатель степени риска (ΣР) рассчитывается по шкале от 0 до 100 и определяется путем суммирования показателей по следующей формуле:

$$\Sigma Р = \Sigma Р_{з} + \Sigma Р_{н}$$

где:

ΣР - общий показатель степени риска;

$\Sigma Р_{з}$ - показатель нарушений значительной степени;

$\Sigma Р_{н}$ - показатель нарушений незначительной степени.

По показателям степени риска проверяемый субъект относится:

1) к высокой степени риска – при показателе степени риска от 60 до 100 и в отношении него проводится выборочная проверка;

2) не отнесенной к высокой степени риска – при показателе степени риска от 0 до 60 и в отношении него не проводится выборочная проверка.

4. Заключительные положения

12. Кратность проведения выборочной проверки составляет 1 раз в год и определяется по результатам проводимого анализа и оценки получаемых сведений по субъективным критериям.

13. Выборочные проверки проводятся на основании списков выборочных проверок, формируемых на полугодие по результатам проводимого анализа и оценки, которые направляются в уполномоченный орган по правовой статистике и специальным учетам в срок не позднее, чем за пятнадцать календарных дней до начала соответствующего отчетного периода.

14. Списки выборочных проверок составляются с учетом:

1) приоритетности проверяемых субъектов (объектов) с наибольшим показателем степени риска по субъективным критериям;

2) нагрузки на должностных лиц, осуществляющих проверки, государственного органа.

Приложение 1
к Критериям оценки степени риска в области связи

Субъективные критерии по информационному источнику «результаты предыдущих проверок (выборочных, внеплановых)»

№	Критерии	Степень нарушени
Результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) (степень тяж устанавливается при несоблюдении нижеперечисленных требований)		

1.	наличие лицензии на предоставление лицензируемых видов услуг в области связи	грубая
2.	обеспечение органам, осуществляющим оперативно-розыскную деятельность на сетях связи, организационные и технические возможности проведения оперативно-розыскных мероприятий на всех сетях связи	грубая
3.	осуществление сбора и хранения в течение двух лет служебной информации об абонентах	грубая
4.	подтверждение соответствия технических средств связи, используемые на единой сети телекоммуникаций Республики Казахстан, радиоэлектронных средств и высокочастотных устройств, являющиеся источником электромагнитного излучения, технических средств почтовой связи	грубая
5.	исполнение предписаний об устранении нарушений в работе отдельных средств или сетей связи охраны труда и техники безопасности, которые создают угрозу жизни и здоровью людей, окружающей среде или нормальному функционированию систем жизнеобеспечения	значительная
6.	наличие системы учета трафика, которая должна иметь систему измерения длительности соединений и систему измерения передачи данных оператора связи, внесенную в реестр государственной системы обеспечения единства измерений Республики Казахстан, имеющую действующий сертификат поверки	значительная
7.	соответствие присоединения к сети телекоммуникаций общего пользования на местном уровне	значительная
8.	соответствие присоединения к сети телекоммуникаций общего пользования на внутризоновом уровне	значительная
9.	соответствие присоединения к сети телекоммуникаций общего пользования на междугородном и международном уровнях	значительная
10.	соответствие присоединения к сети телекоммуникаций общего пользования сетей подвижной связи	значительная
11.	соответствие доступа к узлам телематических служб, интеллектуальных сетей и операторов сетей передачи данных	значительная
12.	соответствие подключения к сети телекоммуникаций общего пользования оборудования (узлов доступа) операторов IP-телефонии (Интернет – телефонии)	значительная
13.	использование оператором связи, провайдером услуги, владельцем ведомственной сети телекоммуникаций, сети телекоммуникаций специального назначения, корпоративной сети выделенного ресурса нумерации местной сети телекоммуникаций в географически определяемой зоне нумерации с кодом «ABC» более чем на 50 процентов в течение двух лет с момента выделения (по результатам проверки, осуществляемой уполномоченным органом, изымается неиспользуемая часть от всей выделенной емкости нумерации)	незначительная
14.	использование получателем ресурса нумерации (коды «DEF» и индексы «X_1», «X_1X_2» в коде «DEF» не географически определяемых зон нумерации, коды операторов ($X_1X_2X_3$/($X_1X_2X_3X_4$), предоставляющих услуги связи с использованием кодов доступа к услуге; номера доступа «1UV (X_1(X_2))» к экстренным оперативным, информационно-справочным и заказным службам; префиксы выбора операторов междугородной и (или) международной связи более чем 6 месяцев в течение двух лет с момента выделения (по результатам проверки, осуществляемой уполномоченным органом)	незначительная
15.	осуществление операторами связи обмена трафиком с зарубежными операторами связи исключительно через операторов междугородной и международной связи Республики Казахстан	грубая

16.	осуществление операторами междугородной и международной связи обмена трафиком с зарубежными операторами связи через Систему Централизованного управления сетями телекоммуникаций	грубая
17.	содержание на сети телекоммуникаций оператора междугородной и (или) международной связи наземных сегментов и коммутационных узлов, центр управления которыми расположен на территории Республики Казахстан	значительная
18.	осуществление резервирования транспортных сетей путем предоставления независимых обходных путей, организуемых по независимым географическим трассам, или замены на тракты (каналы), организуемые в тех же линиях передачи	значительная
19.	наличие в составе СТОММС не менее одной точки стыковки транспортной сети с сетями телекоммуникаций операторов связи зарубежных стран по наземным линиям связи	значительная
20.	наличие в составе СТОММС транспортных сетей телекоммуникаций (магистральных и внутризоновых линии связи)	значительная
21.	наличие в составе СТОММС коммутационных междугородных и международных станций	значительная
22.	наличие в составе СТОММС систем обеспечения функционирования – систему управления и систему технической эксплуатации	значительная
23.	наличие в составе СТОММС системы тактовой сетевой синхронизации	значительная
24.	наличие на транспортных СТОММС сетевых узлов (ПСУ), которые имеют не менее трех выходов (трех направлений) передачи (два в направлении своей сети и один в направлении сети другой страны) для организации международных соединений со СТОП других стран	значительная
25.	самостоятельное создание (развитие) оператором междугородной и международной связи сетей обеспечивающих универсальные услуги телекоммуникаций	значительная
26.	выполнение ОММС мероприятий по мобилизационной готовности	значительная
27.	охват СТОММС территории не менее шести областей (географических зон нумерации), городов Астаны и Алматы	значительная
28.	все МЦК ОММС должны быть связаны не менее чем с двумя МЦК других ОММС, а все АМТС должны быть связаны не менее чем с двумя МЦК	незначительная
29.	наличие квалифицированного состава технических руководителей и специалистов	незначительная
30.	предоставление ОММС информации по распределению пакетов акций (долей участия в уставном капитале) между акционерами (участниками)	незначительная
31.	разработка оператором междугородной и международной связи СТОП на основании полученных заявок, Перечня (трассы) каналов связи, предоставляемых в военное время , с учетом возможности взаимоувязанной сети телекоммуникаций	значительная
32.	соблюдение проверяемым субъектом размеров единиц тарификации, утвержденных приказом Председателя Агентства Республики Казахстан по информатизации и связи от 2 февраля 2009 года № 43	значительная
33.	обеспечение предоставления абонентам бесплатных соединений с экстренной медицинской, правоохранительной, пожарной, аварийной, справочной и другими службами	значительная
34.	уведомление оператором связи абонента до начала тарифицируемого соединения о стоимости данного соединения при оказании интеллектуальных услуг (лотерея, голосование, телевикторина, викторина, справочно-информационные службы, службы знакомств)	значительная
35.	создание системы информационно-справочного обслуживания в целях предоставления абонентам информации, связанной с оказанием услуг связи	незначительная

36.	осуществление автоматического учета информации о полученных абонентом услугах связи в сети оператора связи, времени пользования ими, соединениях с номерами телефонов абонентов других сетей аналогичного стандарта	незначительная
37.	обеспечение технической возможности свободного выбора абонентом оператора междугородной или международной связи	значительная
38.	установка лимита по пересылке абонентам в ночное время (с 22:00 часов до 06:00) информации (рассылок рекламного характера) посредством коротких текстовых сообщений и/или мультимедийных сообщений, не запрошенной ранее абонентом (для сотовых операторов)	незначительная
39.	недопущение навязывания оператором связи абоненту иных платных услуг при оказании ему услуг связи	значительная
40.	принятие в течение трех календарных дней со дня подачи абонентом заявления об ухудшении качества услуг телефонной связи необходимых мер по восстановлению качества и производит перерасчет абонентской платы	незначительная
41.	произведение перерасчета абонентской платы за период фактического бездействия абонентского устройства не по вине абонента	незначительная
42.	информирование абонента об авариях на сетях связи и о предполагаемых сроках устранения этих аварий	незначительная
43.	извещение абонента за 30 календарных дней о замене абонентского номера и (или) об отключении терминала с указанием причин	незначительная
44.	изменение условий тарифа на услуги связи с согласия абонента, известив его об этом не позднее чем за 30 дней до введения их в действие	незначительная
45.	возобновление доступа к услугам связи, отключенным за несвоевременную оплату, в течение двадцати четырех часов с момента погашения задолженности	незначительная
46.	предоставление по требованию абонента информации, связанной с оказанием ему услуг связи	незначительная
47.	недопущение ограничения оператором связи прав абонента/пользователя при оказании ему услуг связи в случае неисполнения им условий получения иной услуги	незначительная
48.	заключение оператором связи либо его представителем договора с абонентами на оказание услуг связи	значительная
49.	ведение реестра операторами связи идентификационных кодов абонентских устройств, работающих в их сети (для сотовых операторов)	незначительная
50.	приостановление либо возобновление по идентификационному коду работу абонентского устройства в своей сети по заявлению собственника абонентского устройства (для сотовых операторов)	значительная
51.	информирование абонентов о профилактическом обслуживании оборудования связи, связанном с его частичным или полным отключением, и о сроках проведения таких работ за десять календарных дней до начала данных работ	незначительная
52.	обеспечение возможности в круглосуточном режиме проверки баланса денег на текущем счете (для сотовых операторов)	незначительная
53.	возвращение абоненту излишне уплаченных денежных средств за оказанные услуги связи или зачитыванию их при согласии абонента в качестве авансирования услуг связи	незначительная
54.	недопущение отказа оператора связи от заключения договора об оказании услуг связи при наличии технической возможности	значительная
55.	замена абонентских номеров в связи с изменением плана нумерации сетей связи без взимания дополнительной платы с предварительным уведомлением абонентов о причине такой замены	незначительная
56.	соблюдение условий кредитного способа оплаты услуг связи	незначительная

57.	соблюдение условий авансового способа оплаты услуг связи	незначительная
58.	сохранение абонентского номера за абонентом в течение двенадцати месяцев с момента окончания на лицевом счете денег абонента	незначительная
59.	осуществление по обращению абонентов перерегистрации абонента без взимания дополнительной оплаты	незначительная
60.	соблюдение сроков доставки почтовых отправлений, утвержденных приказом Председателя Агентства Республики Казахстан по информатизации и связи от 4 марта 2004 года № 48	незначительная
61.	недопущения утраты, недостачи, повреждения (порчи) регистрируемых почтовых отправлений	незначительная
62.	недопущения искажения текста телеграммы, изменившее ее смысл	незначительная

Примечание: расшифровка аббревиатуры:

1. СТОММС - сеть телекоммуникаций оператора междугородной и (или) международной связи;
2. ПСУ – пригранычный сетевой узел;
3. СТОП - сети телекоммуникаций общего пользования;
4. ОММС - оператор междугородной и (или) международной связи;
5. МЦК - международный центр коммутации;
6. АМТС - автоматическая междугородная телефонная станция.

Приложение 2
к Критериям оценки степени риска в области связи

Субъективные критерии по информационному источнику «результаты мониторинга радиочастотного спектра, радиоэлектронных средств и (или) высокочастотных устройств, качества предоставляемых услуг связи »

№	Критерии	Степень нарушения
1.	наличие разрешений на использование радиочастотного спектра Республики Казахстан либо разрешения судовой станции на использование радиочастотного спектра	грубая
2.	наличие разрешений на эксплуатацию радиоэлектронных средств и высокочастотных устройств	значительная
3.	соответствие технических характеристик и условий эксплуатации радиоэлектронных средств и высокочастотных устройств требованиям, изложенным в разрешениях	значительная
4.	предоставление пользователям услуг связи соответствующих по качеству Показателям качества услуг связи	незначительная

Приложение 3
к Критериям оценки степени риска в области связи

Субъективные критерии по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов»

№	Критерии	Степень нарушения
1.	наличие одной подтвержденной жалобы или обращения в области связи	незначительное
2.	наличие двух или более подтвержденных жалоб или обращений в области связи	значительное

Приложение 3
к совместному приказу
Министра по инвестициям и развитию
Республики Казахстан
от 29 июня 2015 года № 735
и исполняющего обязанности
Министра национальной экономики
Республики Казахстан
от 30 июня 2015 года № 494

Критерии оценки степени риска за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи

1. Общие положения

1. Настоящие Критерии оценки степени риска за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи (далее - Критерии) разработаны в соответствии с Законом Республики Казахстан от 6 января 2011 года «О государственном контроле и надзоре в Республике Казахстан» для отнесения проверяемых субъектов к степеням риска и отбора проверяемых субъектов при проведении выборочных проверок.

2. В настоящих Критериях используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства с учетом степени тяжести его последствий;

2) объективные критерии оценки степени риска (далее – объективные критерии) – критерии оценки степени риска, используемые для отбора

проверяемых субъектов (объектов) в зависимости от степени риска в определенной сфере деятельности и не зависящие непосредственно от отдельного субъекта (объекта);

3) субъективные критерии оценки степени риска (далее – субъективные критерии) – критерии оценки степени риска, используемые для отбора проверяемых субъектов (объектов) в зависимости от результатов деятельности конкретного проверяемого субъекта (объекта);

4) система оценки рисков – комплекс мероприятий, проводимый органом контроля и надзора, с целью назначения проверок;

5) проверяемые субъекты за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи (далее – проверяемые субъекты) – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства.

3. Критерии оценки степени риска для выборочных проверок формируются посредством объективных и субъективных критериев.

2. Объективные критерии

4. Определение риска за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи осуществляется в зависимости от вероятности причинения вреда в результате деятельности проверяемого субъекта жизни или здоровью человека, окружающей среде, законным интересам физических и юридических лиц, имущественным интересам государства деятельностью проверяемых субъектов, связанную с бесконтрольным использованием и выдачей электронных документов и электронной цифровой подписи могут привести к компрометации открытого ключа, и как следствие неправомерного использования электронной цифровой подписи.

5. По объективным критериям к высокой степени риска относятся проверяемые субъекты аккредитованные на территории Республики Казахстан удостоверяющие центры.

6. В отношении проверяемых субъектов, отнесенных к высокой степени риска проводятся выборочные проверки.

3. Субъективные критерии

7. Определение субъективных критериев осуществляется с применением следующих этапов:

1) формирование базы данных и сбор информации;

2) анализ информации и оценка рисков.

8. Формирование базы данных и сбор информации необходимы для выявления субъектов контроля, нарушающих законодательство Республики Казахстан об электронном документе и электронной цифровой подписи.

Анализ информации и оценка субъективных критериев позволит сконцентрировать проверки в отношении субъекта контроля с наибольшим потенциальным риском. При этом, при анализе и оценке не применяются данные субъективных критериев, ранее учтенных и использованных в отношении конкретного проверяемого субъекта.

Для оценки степени рисков по субъективным критериям используются следующие источники информации:

1) результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) субъектов контроля. При этом, степень тяжести нарушений (грубое, значительное, незначительное) устанавливается в случае несоблюдения требований законодательства, отраженных в проверочных листах;

2) наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов.

9. Оценка степени риска проверяемых субъектов и отнесение их к высокой или не отнесенным к высокой степени риска по субъективным критериям осуществляется по следующим показателям:

1) по информационному источнику «результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля)» субъективные критерии согласно приложению 1 к настоящим Критериям;

2) по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов» субъективные критерии согласно приложению 2 к настоящим Критериям.

10. Определение степени риска по каждому информационному источнику определяется следующим образом.

Одно невыполненное требование грубой степени приравнивается к показателю 100 и это является основанием для проведения проверки в выборочном порядке.

В случае если нарушение требований грубой степени не выявлено, то для определения показателя степени риска рассчитывается суммарный показатель требований значительной и незначительной степени.

При определении показателя нарушений значительной степени применяется коэффициент 0,7 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_з = (\Sigma P_2 \times 100 / \Sigma P_1) \times 0,7$$

где:

$\Sigma P_з$ – показатель нарушений значительной степени;

ΣP_1 – общее количество индикаторов значительной степени, предъявленных к проверке (анализу) проверяемому субъекту (объекту);

ΣP_2 - количество нарушенных требований значительной степени.

При определении показателя нарушений незначительной степени применяется коэффициент 0,3 и данный показатель рассчитывается по следующей формуле:

$$\Sigma P_н = (\Sigma P_2 \times 100 / \Sigma P_1) \times 0,3$$

где:

$\Sigma P_н$ – показатель нарушений незначительной степени;

ΣP_1 – общее количество индикаторов незначительной степени, предъявленных к проверке (анализу) проверяемому субъекту (объекту);

ΣP_2 - количество нарушенных требований незначительной степени.

Общий показатель степени риска (ΣP) рассчитывается по шкале от 0 до 100 и определяется путем суммирования показателей по следующей формуле:

$$\Sigma P = \Sigma P_з + \Sigma P_н$$

где:

ΣP - общий показатель степени риска;

$\Sigma P_з$ - показатель нарушений значительной степени;

$\Sigma P_н$ - показатель нарушений незначительной степени.

По показателям степени риска проверяемый субъект (объект) относится:

1) к высокой степени риска – при показателе степени риска от 60 до 100 и в отношении него проводится выборочная проверка;

2) не отнесенной к высокой степени риска – при показателе степени риска от 0 до 60 и в отношении него не проводится выборочная проверка.

4. Заключительные положения

11. Кратность проведения выборочной проверки составляет 1 раз в год и определяется по результатам проводимого анализа и оценки получаемых сведений по субъективным критериям.

12. Выборочные проверки проводятся на основании списков выборочных проверок, формируемых на полугодие по результатам проводимого анализа и оценки, которые направляются в уполномоченный орган по правовой статистике и специальным учетам в срок не позднее, чем за пятнадцать календарных дней до начала соответствующего отчетного периода.

13. Списки выборочных проверок составляются с учетом:

1) приоритетности проверяемых субъектов (объектов) с наибольшим показателем степени риска по субъективным критериям;

2) нагрузки на должностных лиц, осуществляющих проверки, государственного органа.

Приложение 1
к Критериям оценки степени риска
за соблюдением законодательства
Республики Казахстан об электронном
документе и электронной цифровой подписи

Субъективные критерии по информационному источнику «результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля)»

№	Критерии	Степень нарушен
Результаты анализа предыдущих проверок (выборочных, внеплановых и иных форм контроля) (степень тяж устанавливается при несоблюдении нижеперечисленных требований)		
1.	наличие процедуры синхронизации времени аккредитуемого удостоверяющего центра с комплексом технических средств, обеспечивающих периодическую передачу цифровой информации о значении текущего времени от эталона единицы времени Республики Казахстан, спутниковых глобальных систем позиционирования, общепризнанных международных источников	грубая
2.	наличие сертификата соответствия на используемые СКЗИ по СТ РК 1073-2007, которые применяется в данном удостоверяющем центре и его пользователями	грубая
3.	наличие аттестата соответствия удостоверяющего центра требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам, в случае интеграции аккредитуемого удостоверяющего центра с государственными информационными системами	значительная
4.	соблюдение требований владельца по отзыву регистрационного свидетельства	грубая
5.	соблюдение требований к серверному помещению	грубая
6.	наличие политики информационной безопасности удостоверяющего центра	незначительная
7.	наличие регламента или правил деятельности удостоверяющего центра	значительная
8.	наличие политики применения регистрационных свидетельств	незначительная
9.	наличие положения об удостоверяющем центре	значительная
10.	наличие инструкции по действиям работников, осуществляющих работы от лица заявителя непосредственно участвующих в работах по сопровождению, администрированию, выпуску	незначительная

	регистрационных свидетельств удостоверяющего центра во внештатных, кризисных ситуациях	
11.	наличие инструкции о резервном копировании информационных ресурсов удостоверяющего центра	грубая
12.	наличие инструкции по установке и настройке программного обеспечения удостоверяющего центра	значительная
13.	наличие в регистрационном свидетельстве номера регистрационного свидетельства и срок его действия	значительная
14.	наличие в регистрационном свидетельстве данных, позволяющих идентифицировать владельца электронной цифровой подписи	значительная
15.	наличие в регистрационном свидетельстве открытого ключа электронной цифровой подписи	значительная
16.	наличие в регистрационном свидетельстве данных о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи	значительная
17.	наличие в регистрационном свидетельстве информации о сферах применения и ограничениях применения электронной цифровой подписи	значительная
18.	наличие в регистрационном свидетельстве реквизитов соответствующего удостоверяющего центра	значительная
19.	наличие схемы взаимодействия модулей (компонент) удостоверяющего центра и схемы электронной цифровой подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной цифровой подписи и требованиями к отдельным параметрам и удостоверяющему центру, утвержденные заявителем	значительная
20.	отсутствие фактов некорректного использования электронной цифровой подписи	значительная

Приложение 2
к Критериям оценки степени риска
за соблюдением законодательства
Республики Казахстан об электронном
документе и электронной цифровой подписи

Субъективные критерии по информационному источнику «наличие и количество подтвержденных жалоб и обращений на проверяемые субъекты, поступивших от физических или юридических лиц, государственных органов»

№	Критерии	Степень нарушен
1.	наличие одной подтвержденной жалобы или обращения за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи	незначительное
2.	наличие двух или более подтвержденных жалоб или обращений за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи	значительное

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан»
Министерства юстиции Республики Казахстан