**Об утверждении критериев оценки степени риска в области информатизации и связи**

*Утративший силу*

Совместный приказ Председателя Агентства Республики Казахстан по информатизации и связи от 17 февраля 2010 года № 65 и Министра экономики и бюджетного планирования Республики Казахстан от 19 февраля 2010 года № 88. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 февраля 2010 года № 6091. Утратил силу совместным приказом Министра связи и информации Республики Казахстан от 31 августа 2011 года № 263 и и.о. Министра экономического развития и торговли Республики Казахстан от 16 сентября 2011 года № 305

Сноска. Утратил силу совместным приказом Министра связи и информации РК от 31.08.2011 № 263 и и.о. Министра экономического развития и торговли РК от 16.09.2011 № 305 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Примечание РЦПИ!

Порядок введения в действие совместного приказа см. п. 4.

В целях реализации пункта 2 статьи 38 Закона Республики Казахстан "О частном предпринимательстве" **ПРИКАЗЫВАЕМ**:

1. Утвердить:

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

2) Критерии оценки степени риска в области связи согласно приложению 2 к настоящему приказу.

2. Департаментам связи, информационных технологий Агентства Республики Казахстан по информатизации и связи (Баймуратов А.Е., Елеусизова К.Б.) в установленном законодательном порядке:

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

2) после государственной регистрации настоящего приказа обеспечить его официальное опубликование и размещение на интернет-ресурсе Агентства Республики Казахстан по информатизации и связи.

3. Контроль за исполнением настоящего приказа возложить на ответственного секретаря Агентства Республики Казахстан по информатизации и связи Маханбетажиева Б.А.

4. Настоящий приказ вступает в силу со дня государственной регистрации и вводится в действие со дня его первого официального опубликования.

*Председатель Агентства Республики Казахстан по информатизации и связи*

_____ *К. Есекеев*

*Министр экономики и бюджетного планирования Республики Казахстан*

_____ *Б. Султанов*

Приложение № 1
к совместному приказу
Председателя Агентства
Республики Казахстан
по информатизации и связи
от 17 февраля 2010 года № 65
и Министра экономики и
бюджетного планирования
Республики Казахстан
от 19 февраля 2010 года № 88

## Критерии
## оценки степени риска в области информатизации

1. Настоящие Критерии оценки степени риска в сфере информатизации ( далее - Критерии) разработаны в соответствии с Законами Республики Казахстан "О частном предпринимательстве", "Об информатизации", "Об электронном документе и электронной цифровой подписи".

2. Настоящие Критерии определяют совокупность количественных и качественных показателей риска, на основании которых осуществляется отнесение субъектов информатизации к различным степеням риска.

3. В настоящих Критериях используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности субъектов информатизации законным интересам личности, общества, государства, с учетом степени тяжести его последствий, а именно:

при использовании электронных информационных ресурсов и информационных технологий;

финансовый ущерб государству либо физическому лицу за счет использования контрольно-кассовых машин, являющихся компьютерной системой, неразрешенных к использованию на территории Республики Казахстан ;

2) субъекты информатизации (Субъекты)- центральные и местные исполнительные органы, удостоверяющие центры, владельцы государственных

информационных ресурсов и информационных систем, поставщики информации, кредитных бюро и получателей кредитных историй, владельцы контрольно-кассовых машин, являющихся компьютерной системой, владельцы негосударственных информационных систем, интегрируемых с государственными информационными системами.

4. Первично Субъекты относятся к высокой степени риска.

5. После проверки Субъекты распределяются по степени риска в соответствии с Качественными показателями оценки степени риска (далее - Качественные показатели) и при их наличии присваивается соответствующий балл, согласно приложению к настоящим Критериям.

6. В случае, если действие или бездействие Субъекта подпадает под действие нескольких Качественных показателей, то баллы суммируются.

7. Баллы по Качественным показателям суммируются для определения общего суммарного итога.

8. Результаты суммарного итога используются для дифференциации Субъектов по степеням риска.

9. Дифференциация Субъектов по степеням риска осуществляется следующим образом:

к группе высокого риска относятся Субъекты, набравшие от 20 и более баллов;

к группе среднего риска - от 11 до 20 баллов;

к группе незначительного риска - от 0 до 10 баллов.

10. Отбор Субъектов внутри одной группы риска осуществляется уполномоченным органом в сфере информатизации следующим образом:

1) наибольший непроверенный период (при определении непроверенного периода не учитываются внеплановые тематические проверки);

2) наибольшая сумма баллов;

3) количество информационных ресурсов и информационных систем.

Приложение к Критериям оценки степени риска в сфере информатизации

**Качественные показатели оценки степени риска**

| № | Нарушения требований, установленных Законами Республики Казахстан и постановлениями Правительства Республики Казахстан | Условия присвоения баллов | Б л |
|---|---|---|---|
| | показатели в сфере обеспечения информационной безопасности | | |
| 1 | Несанкционированный доступ к конфиденциальной и служебной информации | да | 2 |
| | | нет | 0 |
| 2 | Нелегитимное использование средств криптографической защиты информации | да | 2 |
| | | нет | 0 |

| | | | |
|---|---|---|---|
| 3 | Компрометация закрытого ключа удостоверяющего центра | да | 2 |
| | | нет | 0 |
| 4 | Наличие уязвимостей по информационной безопасности в информационных ресурсах государственных органов | да | 2 |
| | | нет | 0 |
| 5 | Нарушение требований по интеграции государственных информационных систем с негосударственными информационными системами | да | 2 |
| | | нет | 0 |
| 6 | Не соответствие квалификационным требованиям, предъявляемым к деятельности удостоверяющих центров | да | 2 |
| | | нет | 0 |
| 7 | Нарушение порядка эксплуатации электронных информационных ресурсов и информационных систем | да | 1 |
| | | нет | 0 |
| 8 | Отсутствие организационной и нормативно-технической документации по обеспечению информационной безопасности | да | 1 |
| | | нет | 0 |
| 9 | Использование несертифицированных технических средств и программных продуктов | да | 1 |
| | | нет | 0 |
| 10 | Несвоевременное внесение изменений и дополнений в базу данных по действительным, отозванным и аннулированным сертификатам | да | 1 |
| | | нет | 0 |
| 11 | Не укомплектованность техникой и программным обеспечением, вследствие чего допущены нарушения требований информационной безопасности | да | 1 |
| | | нет | 0 |
| 12 | Наличие вирусов и вредоносных программ | да | 5 |
| | | нет | 0 |
| 13 | Сбои и отказы в работе корпоративной сети передачи данных, рабочих станций пользователей и серверов | да | 5 |
| | | нет | 0 |
| | показатели в сфере эксплуатации программных продуктов | | |
| 14 | Несоблюдение требований по обязательной регистрации государственных информационных ресурсов и информационных систем и вносимых в них изменений | да | 2 |
| | | нет | 0 |
| 15 | Нарушение требований по включению разработанных и приобретенных на счет бюджетных средств программных продуктов и технических средств в депозитарий информационных систем, программных продуктов, программных кодов и нормативно-технической документации (далее - Депозитарий) | да | 2 |
| | | нет | 0 |
| 16 | Потеря информации при передаче данных из-за сбоев в работе программного обеспечения | да | 2 |
| | | нет | 0 |
| 17 | Закладки и недекларированные возможности программного обеспечения | да | 2 |
| | | нет | 0 |
| 18 | Не внесение изменений и дополнений информационных систем, программных продуктов, | да | 1 |

| | | | |
|---|---|---|---|
| | программных кодов и нормативно-технической документации в Депозитарий | нет | 0 |
| 19 | Несоответствие нормативно-технической документации информационных ресурсов, информационных систем и программных продуктов стандартным требованиям по комплектности, содержанию и оформлению | да | 1 |
| | | нет | 0 |
| 20 | Функциональное несоответствие программного обеспечения заявленным требованиям | да | 1 |
| | | нет | 0 |
| 21 | Соответствие качества программного обеспечения требованиям стандартов Республики Казахстан | да | 0 |
| | | нет | 1 |
| 22 | Утрата нормативно-технической документации на разработанные или приобретенные за счет государственных средств электронных информационных ресурсов, информационных систем и программного обеспечения | да | 5 |
| | | нет | 0 |
| 23 | Отсутствие персонала и нормативно-технической документации для сопровождения программного обеспечения | да | 5 |
| | | нет | 0 |
| 24 | Утрата установочных пакетов программных продуктов | да | 5 |
| | | нет | 0 |
| | показатели владельцев контрольно-кассовых машин являю компьютерной системой и поставщиков информации, кредитных и получателей кредитных отчетов | | |
| 25 | Отсутствие сертифицированных средств криптографической защиты информации | да | 2 |
| | | нет | 0 |
| 26 | Несоблюдение требований к серверному помещению и помещению ограниченного доступа | да | 2 |
| | | нет | 0 |
| 27 | Отсутствие системы защиты от несанкционированного доступа | да | 2 |
| | | нет | 0 |
| 28 | Использование не сертифицированных на соответствие требованиям информационной безопасности технических и программных средств | да | 2 |
| | | нет | 0 |
| 29 | Отсутствие системы защиты объекта от утечки информации по техническим каналам | да | 2 |
| | | нет | 0 |
| 30 | Несоблюдение требований к рабочему месту пользователя | да | 1 |
| | | нет | 0 |
| 31 | Отсутствие модуля «рабочее место налогового инспектора» | да | 1 |
| | | нет | 0 |
| 32 | Отсутствие средств идентификации и аутентификации пользователей | да | 1 |
| | | нет | 0 |
| 33 | Отсутствие средств проверки целостности системы | да | 1 |
| | | нет | 0 |
| 34 | Отсутствие лицензий на программное и аппаратное обеспечение | да | 1 |
| | | нет | 0 |

| | | | |
|---|---|---|---|
| 35 | Отсутствие системы резервного копирования и архивирования данных | да | 1 |
| | | нет | 0 |
| 36 | Непринятие мер по разграничению доступа к ресурсам | да | 5 |
| | | нет | 0 |
| 37 | Отсутствие паспорта рабочего места | да | 5 |
| | | нет | 0 |
| 38 | Отсутствие технической документации, регламенти-рующей организацию информационного процесса | да | 5 |
| | | нет | 0 |
| 39 | Отсутствие инструкции по обеспечению информа-ционной безопасности рабочего места пользователя | да | 5 |
| | | нет | 0 |

Приложение № 2
к совместному приказу
Председателя Агентства
Республики Казахстан
по информатизации и связи
от 17 февраля 2010 года № 65
и Министра экономики и
бюджетного планирования
Республики Казахстан
от 19 февраля 2010 года № 88

## Критерии оценки степени риска в области связи

1. Настоящие Критерии оценки степени риска в области связи (далее - Критерии) разработаны в соответствии с Законами Республики Казахстан "О частном предпринимательстве", "О связи".

2. Настоящие Критерии определяют совокупность количественных и качественных показателей риска, на основании которых осуществляется отнесение субъектов в области связи к различным степеням риска.

3. В настоящих Критериях используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности Субъектов в области связи законным интересам физических и юридических лиц и государства, общества с учетом степени тяжести его последствий, а именно:

бесконтрольное использование платного ограниченного ресурса радиочастотного спектра, которое может привести к недопоступлению обязательных платежей в государственный бюджет;

использование радиочастотного спектра без разрешительных документов, которое может привести к возникновению радиопомех и невозможности использования его законными владельцами;

эксплуатация оборудования на сетях телекоммуникаций без технических

средств проведения специальных оперативно-розыскных мероприятий, которая может привести к невозможности проведения органами оперативно-розыскной деятельности необходимых мероприятий;

2) субъект контроля - оператор связи (физическое или юридическое лицо, получившее лицензию на предоставление услуг связи); хозяйствующие субъекты , осуществляющие деятельность в области связи (операторы связи, владельцы специальных, ведомственных и корпоративных сетей телекоммуникаций, отдельного коммутационного оборудования, подключаемого к сети телекоммуникаций общего пользования, владельцы радиоэлектронных средств, являющиеся пользователями радиочастотным спектром); государственные учреждения, использующие радиочастотный спектр в производственных целях.

4. Отнесение субъектов контроля к степени рисков осуществляется в два этапа:

первый этап - на основании объективных критериев степени риска;

второй этап - на основании субъективных критериев степени риска.

5. Объективные критерии степени риска:

1) к высокой степени группы риска отнесены - субъекты, получившие лицензии на предоставление следующих услуг связи: междугородная, международная, сотовая; а также местная и передача данных имеющих радиочастотный спектр для предоставления услуг связи;

2) к средней степени группы риска отнесены - субъекты, получившие лицензии на предоставление следующих услуг связи: передача данных, IP-телефония, местная посредством проводной связи, телекоммуникации по выделенной сети связи, спутниковая подвижная связь, мобильная телекоммуникационная связь, предоставление каналов связи, почтовая связь;

3) к незначительной степени группы риска отнесены - государственные учреждения, хозяйствующие субъекты, использующие радиочастотный спектр в производственных целях.

6. Субъективные критерии оценки степени риска подразделяются на:

грубые нарушения;

значительные нарушения;

незначительные нарушения.

7. К грубым нарушениям относятся:

1) предоставление дополнительных услуг связи без соответствующей лицензии;

2) использование радиочастотного спектра и ресурса нумерации без разрешительных документов либо нарушение принципа нумерации;

3) отсутствие технических средств проведения специальных оперативно-розыскных мероприятий на телекоммуникационном оборудовании.

8. К значительным нарушениям относятся:

1) использование не сертифицированного оборудования;

2) эксплуатация радиоэлектронных средств и высокочастотных устройств без разрешения на эксплуатацию;

3) нарушения порядка присоединения к сети телекоммуникаций общего пользования;

4) отсутствие разрешения на ввоз радиоэлектронных средств и высокочастотных устройств на территорию Республики Казахстан;

5) непродление сроков действия разрешения на использование радиочастотного спектра;

6) отсутствие регистрации радиоэлектронных средств.

9. К незначительным нарушениям относится непродление сроков действия разрешения на эксплуатацию на радиоэлектронное средство и высокочастотное устройство.

10. Определение степени риска и распределение по группам степени риска субъектов в области связи для осуществления плановых проверок будет осуществляться ежегодно.

11. Распределение субъектов в области связи по степени риска будет осуществляться на основе анализа по результатам предыдущих проверок (за предшествующий год).

12. Субъекты регулирования, входящие в незначительную степень риска, при совершении в течение проверяемого периода до двух грубых или более двух значительных нарушений переводятся в среднюю степень риска, а при совершении трех грубых нарушений - в высокую степень риска.

13. Субъекты регулирования, входящие в среднюю степень риска, при совершении в течение проверяемого периода одного и более грубых или двух и более значительных нарушений переводятся в высокую степень риска.

14. При невыявлении последней плановой проверкой нарушений, субъекты регулирования переводятся в группу незначительной степени риска.

15. Субъекты высокой или средней группы риска в зависимости от соблюдения требований норм законодательства в области связи будет переводиться из одной группы в другую и, соответственно, будет меняться периодичность их проверки.

16. Отбор субъектов внутри одной степени риска осуществляется уполномоченным органом в области связи следующим образом:

1) наибольший непроверенный период (при определении непроверенного периода не берутся в расчет внеплановые тематические проверки);

2) степень тяжести выявленных нарушений за прошедший период;

3) наличие наибольшего количества радиоэлектронных средств.