О внесении изменений и дополнений в совместный приказ Председателя Комитета национальной безопасности Республики Казахстан от 25 октября 2016 года № 72 и Министра национальной экономики Республики Казахстан от 9 ноября 2016 года № 471 "Об утверждении критериев оценки степени риска и проверочных листов в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий"

Совместный приказ Председателя Комитета национальной безопасности Республики Казахстан от 24 мая 2023 года № 32/қе и Министра национальной экономики Республики Казахстан от 25 мая 2023 года № 80. Зарегистрирован в Министерстве юстиции Республики Казахстан 25 мая 2023 года № 32581

ПРИКАЗЫВАЕМ:

1. Внести в совместный приказ Председателя Комитета национальной безопасности Республики Казахстан от 25 октября 2016 года № 72 и Министра национальной экономики Республики Казахстан от 9 ноября 2016 года № 471 "Об утверждении критериев оценки степени риска и проверочных листов в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 14509) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с пунктом 5 статьи 141 и пунктом 1 статьи 143 Предпринимательского кодекса Республики Казахстан **ПРИКАЗЫВАЕМ:**";

в пункте 1:

подпункт 5) изложить в следующей редакции:

"5) проверочный лист в отношении субъектов (объектов) контроля, осуществляющих деятельность по ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, согласно приложению 5 к настоящему совместному приказу;";

дополнить подпунктами 6), 7) в следующей редакции:

"6) проверочный лист в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности согласно приложению 6 к настоящему совместному приказу;

7) проверочный лист в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности согласно приложению 7 к настоящему совместному приказу.";

приложения 1, 2, 3, 4 и 5 изложить в новой редакции согласно приложениям 1, 2, 3, 4 и 5 к настоящему совместному приказу;

дополнить приложениями 6 и 7 согласно приложениям 6 и 7 к настоящему совместному приказу.

2. Службе информации и кибербезопасности Комитета национальной безопасности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) размещение настоящего совместного приказа на интернет-ресурсе Комитета национальной безопасности Республики Казахстан.

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

Министр национальной экономики Республики Казахстан — *А. Куантыров*

Председатель Комитета национальной безопасности Республики Казахстан — *Е. Сагимбаев*

"СОГЛАСОВАН"
Комитет по правовой
статистике и специальным
учетам Генеральной прокуратуры
Республики Казахстан

Приложение к приказу
Министр национальной
экономики Республики
Казахстан от 25 мая 2023 года
№ 80 и Председателя Комитета
национальной безопасности
Республики Казахстан
от 24 мая 2023 года № 32/қе

Приложение 1
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной

экономики Республики Казахстан
от 9 ноября 2016 года № 471

Критерии
оценки степени риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Глава 1. Общие положения

1. Настоящие Критерии оценки степени риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, (далее – Критерии) разработаны в соответствии с пунктом 5 статьи 141 Предпринимательского кодекса Республики Казахстан, Правилами формирования, регулирующими государственными органами системы оценки и управления рисками, утвержденными приказом исполняющего обязанности Министра национальной экономики Республики Казахстан от 22 июня 2022 года № 48 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 28577), с целью проведения проверок, проводимых на соответствие квалификационным требованиям по выданным лицензиям (далее – проверки на соответствие требованиям).

2. В настоящих Критериях используются следующие понятия:

1) субъекты (объекты) контроля – лицензиаты, осуществляющие деятельность в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий;

2) балл – количественная мера исчисления риска;

3) незначительное нарушение – нарушение требований, установленных нормативными правовыми актами в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в части передачи в постоянное или временное пользование разработанной методики третьим лицам без согласования с лицензиаром;

4) нормализация данных – статистическая процедура, предусматривающая приведение значений, измеренных в различных шкалах, к условно общей шкале;

5) значительное нарушение – нарушение требований, установленных законодательством Республики Казахстан в сферах информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в части несоответствия квалификационным требованиям: представление электронного отчета не по форме, предоставление недостоверных данных в электронном формате, отсутствие разработанных и утвержденных методик, нарушение порядка передачи поисковых технических средств, несоответствие помещения требованиям, предъявляемым к нему;

6) грубое нарушение – нарушение требований, установленных законодательством Республики Казахстан в сферах информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, влекущих административную ответственность, предусмотренную Кодексом Республики Казахстан "Об административных правонарушениях", в части несоответствия квалификационным требованиям: непредставление электронного отчета, отсутствие специалиста, отсутствие специально выделенного помещения для осуществления заявленного вида деятельности, отсутствие разрешения на работу со сведениями, составляющими государственные секреты, отсутствие минимально необходимого оборудования, нарушение порядка уведомления лицензиара, нарушение порядка передачи разработанных, реализуемых или ремонтируемых специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, и документации к ним третьим лицам;

7) риск – вероятность причинения вреда в результате деятельности субъекта контроля законным интересам физических и юридических лиц, имущественным интересам государства с учетом степени тяжести его последствий;

8) система оценки и управления рисками – процесс принятия управленческих решений, направленных на снижение вероятности наступления неблагоприятных факторов путем распределения субъектов (объектов) контроля по степеням риска для последующего осуществления проверок на соответствие требованиям с целью минимально возможной степени ограничения свободы предпринимательства, обеспечивая при этом допустимый уровень риска в соответствующих сферах деятельности, а также направленных на изменение уровня риска для конкретного субъекта (объекта) контроля и (или) освобождения такого субъекта (объекта) контроля от проверок на соответствие требованиям;

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

10) критерии оценки степени риска – совокупность количественных и качественных показателей, связанных с непосредственной деятельностью субъекта контроля, особенностями отраслевого развития и факторами, влияющими на это развитие, позволяющих отнести субъекты (объекты) контроля к различным степеням риска;

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

12) проверочный лист – перечень требований, предъявляемых к деятельности субъектов (объектов) контроля, несоблюдение которых влечет за собой угрозу законным интересам физических и юридических лиц, государства.

Глава 2. Порядок формирования системы оценки и управления рисками при проведении проверки на соответствие требованиям

3. В целях управления рисками при осуществлении проверки на соответствие требованиям в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, критерии оценки степени риска формируются посредством поэтапного определения объективных и субъективных (Мультикритериальный анализ решений).

На первом этапе по объективным критериям субъекты (объекты) контроля относят к одной из следующих степеней риска:

1) высокий риск;

2) средний риск;

3) низкий риск.

Для сфер деятельности субъектов (объектов) контроля, отнесенных к высокой, средней и низкой степени риска, проводятся проверка на соответствие требованиям и внеплановая проверка.

На втором этапе по субъективным критериям субъекты (объекты) контроля относят к одной из следующих степеней риска:

1) высокий риск;

2) средний риск;

3) низкий риск.

По показателям степени риска по субъективным критериям субъект (объект) контроля относится:

1) к высокой степени риска – при показателе степени риска от 71 до 100 включительно;

2) к средней степени риска – при показателе степени риска от 31 до 70 включительно;

3) к низкой степени риска – при показателе степени риска от 0 до 30 включительно.

4. В зависимости от возможного риска и значимости проблемы, единичности или системности нарушения, анализа принятых ранее решений по каждому источнику информации определяются субъективные критерии, которые в соответствии с критериями оценки степени риска соответствуют степени нарушения: грубое, значительное и незначительное.

При формировании субъективных критериев степень нарушения (грубое, значительное, незначительное) присваивается в соответствии с установленными определениями грубых, значительных, незначительных нарушений.

5. Критерии оценки степени риска для проведения проверки на соответствие требованиям формируются посредством объективных и субъективных критериев.

Параграф 1. Объективные критерии

6. Определение объективных критериев осуществляется посредством определения риска.

7. По объективным критериям субъекты (объекты) контроля в сферах информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, распределяются на высокую, среднюю и низкую степени риска в зависимости от наступления неблагоприятного происшествия для законных интересов физических и юридических лиц, государства:

1) к высокой степени риска относятся субъекты (объекты) контроля, осуществляющие деятельность по разработке, производству, ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также субъекты (объекты) контроля, осуществляющие деятельность по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности;

2) к средней степени риска относятся субъекты (объекты) контроля, осуществляющие деятельность по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также субъекты (объекты) контроля, осуществляющие деятельность по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности;

3) к низкой степени риска относятся субъекты (объекты) контроля, осуществляющие деятельность по разработке средств криптографической защиты информации.

Параграф 2. 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 субъектов (объектов) контроля, нарушающих законодательство Республики Казахстан

в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.

Для оценки степени риска используются следующие источники информации:

1) результаты предыдущих проверок;

2) результаты мониторинга отчетности и сведений, представляемых субъектом (объектом) контроля;

3) результаты анализа сведений, представляемых государственными органами.

10. Анализ и оценка субъективных критериев позволяют сконцентрировать проведение проверки на соответствие требованиям субъекта (объекта) контроля в отношении субъекта (объекта) контроля с наибольшим потенциальным риском.

При этом при анализе и оценке не применяются данные субъективных критериев, ранее учтенные и использованные в отношении конкретного субъекта (объекта) контроля, либо данные, по которым истек срок исковой давности в соответствии с законодательством Республики Казахстан.

В отношении субъектов контроля, устранивших в полном объеме выданные нарушения по итогам проведенной предыдущей проверки на соответствие требованиям , не допускается включение их при формировании графиков и списков на очередной период государственного контроля.

11. Степени нарушений требований, предъявляемых к деятельности субъектов (объектов) контроля, устанавливаются согласно приложению 1 к настоящим Критериям.

12. Приоритетность применяемых источников информации и значимость показателей субъективных критериев устанавливаются согласно перечню субъективных критериев для определения степени риска:

1) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке средств криптографической защиты информации, приведен в приложении 2 к настоящим Критериям;

2) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, приведен в приложении 3 к настоящим Критериям;

3) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности

оперативного центра информационной безопасности, приведен в приложении 4 к настоящим Критериям;

4) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности, приведен в приложении 5 к настоящим Критериям;

5) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке и производству специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, приведен в приложении 6 к настоящим Критериям;

6) перечень субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля в отношении субъектов (объектов) контроля, осуществляющих деятельность по ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, приведен в приложении 7 к настоящим Критериям.

Параграф 3. Особенности формирования системы оценки и управления рисками

13. Система оценки и управления рисками ведется с использованием информационных систем, относящих субъекты (объекты) контроля к конкретным степеням риска и формирующих графики.

При отсутствии информационной системы оценки и управления рисками минимально допустимый порог количества субъектов (объектов) контроля, в отношении которых осуществляется проверка на соответствие требованиям, не должен превышать пяти процентов от общего количества таких субъектов контроля в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.

Глава 3. Порядок расчета степени риска по субъективным критериям

14. Расчет показателя степени риска по субъективным критериям (R) осуществляется в автоматизированном режиме путем суммирования показателя

степени риска по нарушениям по результатам предыдущих проверок субъектов (объектов) контроля (SP) и показателя степени риска по субъективным критериям (SC) с последующей нормализацией значений данных в диапазоне от 0 до 100 баллов.

Rпром = SP + SC, где

Rпром – промежуточный показатель степени риска по субъективным критериям,

SP – показатель степени риска по нарушениям,

SC – показатель степени риска по субъективным критериям, определенным в соответствии с пунктом 12 настоящих Критериев.

Расчет производится по каждому субъекту (объекту) контроля однородной группы субъектов (объектов) контроля каждой сферы государственного контроля. При этом перечень оцениваемых субъектов (объектов) контроля, относимых к однородной группе субъектов (объектов) контроля одной сферы государственного контроля, образует выборочную совокупность (выборку) для последующей нормализации данных .

15. По данным, полученным по результатам предыдущих проверок, формируется показатель степени риска по нарушениям, оцениваемый в баллах от 0 до 100.

При выявлении одного грубого нарушения по любому из источников информации, указанных в пункте 11 настоящих Критериев, субъекту контроля приравнивается показатель степени риска 100 баллов и в отношении него проводится проверка на соответствие требованиям.

При невыявлении грубых нарушений показатель степени риска рассчитывается суммарным показателем по нарушениям значительной и незначительной степени.

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

SPз = (SP2 x 100/SP1) x 0,7 ,

где:

SPз – показатель значительных нарушений;

SP1 – требуемое количество значительных нарушений;

SP2 – количество выявленных значительных нарушений.

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

SPн = (SP2 x 100/SP1) x 0,3 ,

где:

SPн – показатель незначительных нарушений;

SP1 – требуемое количество незначительных нарушений;

SP2 – количество выявленных незначительных нарушений.

Показатель степени риска по нарушениям (SP) рассчитывается по шкале от 0 до 100 баллов и определяется путем суммирования показателей значительных и незначительных нарушений по следующей формуле:

SP = SPз + SPн ,

где:

SP – показатель степени риска по нарушениям;

SPз – показатель значительных нарушений;

SPн – показатель незначительных нарушений.

Полученное значение показателя степени риска по нарушениям включается в расчет показателя степени риска по субъективным критериям.

16. Расчет показателя степени риска по субъективным критериям, определенным в соответствии с пунктом 12 настоящих Критериев, производится по шкале от 0 до 100 баллов и осуществляется по следующей формуле:

$$SC = \sum_{i=1}^{n} x_i * w_i, \text{ где}$$

x_i

– показатель субъективного критерия,

w_i

– удельный вес показателя субъективного критерия

x_i,

n– количество показателей.

Полученное значение показателя степени риска по субъективным критериям, определенным в соответствии с пунктом 12 настоящих Критериев, включается в расчет показателя степени риска по субъективным критериям.

17. Рассчитанные по субъектам (объектам) значения по показателю нормализуются в диапазоне от 0 до 100 баллов. Нормализация данных осуществляется по каждой выборочной совокупности (выборке) с использованием следующей формулы:

$$R = \frac{R_{\text{пром}} - R_{min}}{R_{max} - R_{min}} \text{ x } 100 \text{ ,}$$

R– показатель степени риска (итоговый) по субъективным критериям отдельного субъекта (объекта) контроля,

R_{max}

– максимально возможное значение по шкале степени риска по субъективным критериям по субъектам (объектам), входящим в одну выборочную совокупность (выборку) (верхняя граница шкалы),

R_{min}

– минимально возможное значение по шкале степени риска по субъективным критериям по субъектам (объектам), входящим в одну выборочную совокупность (выборку) (нижняя граница шкалы),

$R_{\text{пром}}$

– промежуточный показатель степени риска по субъективным критериям, рассчитанный в соответствии с пунктом 14 настоящих Критериев.

18. Для сфер деятельности субъектов (объектов) контроля, отнесенных к высокой степени риска, проверка на соответствие требованиям проводится не чаще одного раза в год.

Для сфер деятельности субъектов (объектов) контроля, отнесенных к средней степени риска, проверка на соответствие требованиям проводится не чаще одного раза в два года.

Для сфер деятельности субъектов (объектов) контроля, отнесенных к низкой степени риска, проверка на соответствие требованиям проводится не чаще одного раза в три года.

Приложение 1
к Критериям оценки степени
риска в сферах обеспечения
информационной безопасности
и специальных технических
средств, предназначенных для
проведения оперативно-
розыскных мероприятий

Степени нарушений требований, предъявляемых к деятельности субъектов (объектов) контроля

№ п/п	Критерии	Степень нарушений
Для субъектов (объектов) контроля, осуществляющих деятельность по разработке средств криптографической защиты информации (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
	Наличие специалиста, имеющего высшее образование по специальности "Математика", " Физика", "Информатика", " Автоматизация и управление", " Информационные системы", " Вычислительная техника и программное обеспечение", "	

1	Математическое и компьютерное моделирование", " Приборостроение", " Электроэнергетика", " Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", "Системы информационной безопасности", или специалиста, имеющего аналогичное зарубежное высшее образование	грубое
2	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)	грубое
3	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом	значительное
4	Уведомление лицензиара о заключенных договорах (контрактах) на разработку средств криптографической защиты информации не менее чем за пять рабочих дней до начала выполнения обязательств	грубое
5	Уведомление лицензиара о самостоятельно (за счет собственных средств) разработанных средств криптографической защиты информации не более чем за пять рабочих дней после разработки	грубое
Для субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные	

1	системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", "Приборостроение", "Электроэнергетика", "Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование	грубое
2	Наличие минимального набора поисковых технических средств: 1) нелинейный локатор (детектор нелинейных переходов); 2) многофункциональный поисковый прибор; 3) мобильный/стационарный комплекс радиомониторинга или сканирующее радиоприемное устройство; 4) радиопеленгатор носимый; 5) обнаружитель скрытых видеокамер; 6) стетоскоп; 7) досмотровый комплект зеркал или эндоскоп; 8) анализатор проводных линий; 9) тепловизор	грубое
3	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)	грубое
4	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом	значительное
	Наличие разработанной и утвержденной лицензиатом по согласованию с лицензиаром:	

5	1) методики проведения работ по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в помещениях и технических средствах; 2) методики оценки эффективности защищенности помещений и технических средств от утечки информации по техническим каналам	значительное
6	Передача в постоянное или временное пользование поисковых технических средств третьим лицам только по согласованию с лицензиаром	грубое
7	Передача в постоянное или временное пользование разработанных методик третьим лицам только по согласованию с лицензиаром	незначительное
8	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ	грубое
9	Уведомление лицензиара о выявленных в ходе оказания услуг специальных технических средствах, предназначенных для проведения оперативно-розыскных мероприятий, в течение трех рабочих дней после факта выявления	грубое
Для субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
	Наличие специалистов, имеющих высшее или профессиональное	

1	техническое образование, прошедших переподготовку, повышение квалификации по направлениям информационной безопасности: 1) не менее трех специалистов, имеющих дипломы о высшем и (или) профессиональном техническом образовании по профилю информационной безопасности (защите информации); 2) не менее двух специалистов, имеющих сертификаты по направлению аудита требованиям международного стандарта ISO 27001; 3) не менее одного специалиста по направлению компьютерной криминалистики (например, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst и другие); 4) не менее одного специалиста по направлению реверс-инжиниринга и (или) анализа вредоносных программ (например, GIAC Reverse Engineering Malware и другие); 5) не менее одного специалиста по направлению этичного хакинга и (или) тестирования на проникновение (например, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester и другие); 6) не менее двух специалистов по направлению администрирования серверных операционных систем (например, Red Hat Certified System Administrator, Microsoft Certified Solutions Associate и другие)	грубое
	Наличие минимального набора поисковых средств: 1) решение класса next-generation firewall или unified threat management; 2) система обнаружения угроз на рабочих станциях и реагирования на них (Endpoint Threat Detection and Response);	

2	3) средство проактивного поиска и обнаружения угроз (Threat Hunting); 4) средство предотвращения утечки информации (DLP); 5) система управления событиями информационной безопасности (SIEM); 6) платформа реагирования на инциденты (IRP); 7) платформа управления информацией об угрозах (Threat Intelligence Platform); 8) средство динамического анализа вредоносных программ типа "песочница"; 9) сетевой сканер; 10) сканер уязвимостей; 11) сканер уязвимостей веб-приложений; 12) средство эксплуатации уязвимостей; 13) внешний Wi-Fi адаптер с направленной антенной	грубое
3	Специально выделенное помещение (на праве собственности или иного законного основания)	грубое
4	Оборудование помещения автоматическими системами охранной и пожарной сигнализации	значительное
5	Осуществление деятельности при условии: 1) наличия разработанной и утвержденной лицензиатом по согласованию с лицензиаром методики оказания услуг по выявлению технических каналов утечки информации и специальных технических средств оперативным центром информационной безопасности; 2) осуществление заявленного вида деятельности в полном соответствии с методикой оказания услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных	значительное

	мероприятий, оперативным центром информационной безопасности	
6	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, оперативным центром информационной безопасности (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ	значительное
Для субъектов (объектов) контроля, осуществляющих деятельность по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
1	Наличие специалистов, имеющих высшее или профессиональное техническое образование, прошедших переподготовку, повышение квалификации по направлениям информационной безопасности: 1) не менее трех специалистов, имеющих дипломы о высшем и (или) профессиональном техническом образовании по профилю информационной безопасности (защите информации); 2) не менее двух специалистов, имеющих сертификаты по направлению аудита требованиям международного стандарта ISO 27001; 3) не менее одного специалиста по направлению компьютерной криминалистики (например, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst и другие); 4) не менее одного специалиста по направлению реверс-инжиниринга и (или) анализа вредоносных	грубое

	программ (например, GIAC Reverse Engineering Malware и другие); 5) не менее одного специалиста по направлению этичного хакинга и (или) тестирования на проникновение (например, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester и другие)	
2	Наличие минимального набора поисковых средств: 1) платформа реагирования на инциденты (IRP); 2) платформа управления информацией об угрозах (Threat Intelligence Platform); 3) Средство статического анализа вредоносных программ; 4) Средство динамического анализа вредоносных программ типа "песочница"	грубое
3	Специально выделенное помещение (на праве собственности или иного законного основания)	грубое
4	Оборудование помещения автоматическими системами охранной и пожарной сигнализации	значительное
5	Осуществление деятельности при условии: 1) наличие разработанной и утвержденной лицензиатом по согласованию с лицензиаром методики оказания услуг по выявлению технических каналов утечки информации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности; 2) осуществление заявленного вида деятельности в полном соответствии с методикой оказания услуг по выявлению технических каналов утечки информации специальных технических средств,	значительное

	предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности	
6	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ	значительное
Для субъектов (объектов) контроля, осуществляющих деятельность по разработке, производству, ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
Подвид деятельности по разработке и производству специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий		
1	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", "Приборостроение", "Электроэнергетика", "Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование	грубое
	Наличие минимального набора технических средств и контрольно-измерительного оборудования: 1) мультиметр; 2) осциллограф; 3) вольтметр; 4) амперметр; 5) частотомер;	

2	6) генератор сигналов высокочастотный; 7) генератор сигналов низкочастотный; 8) источник постоянного тока с регулировкой силы тока и напряжения; 9) источник переменного регулируемого напряжения (автотрансформатор); 10) индикатор поля; 11) паяльная станция	грубое
3	Наличие специально выделенного производственного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)	грубое
4	Наличие специально выделенного помещения для хранения разрабатываемых и произведенных специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий (на праве собственности или ином законном основании)	грубое
5	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом	значительное
	Осуществление разработки специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, на условиях: 1) наличия технического задания на разработку специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, утвержденного	

6	органом, осуществляющим оперативно-розыскную деятельность, и согласованного с лицензиаром; 2) предоставление лицензиару опытного образца разработанного специальных технических средств, предназначенного для проведения оперативно-розыскных мероприятий, для проведения его научно-технической экспертизы	значительное
7	Осуществление производства специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, на условиях: 1) наличия конструкторской документации на производимое специальное техническое средство, предназначенное для проведения оперативно-розыскных мероприятий, утвержденной органом, осуществляющим оперативно-розыскную деятельность, и согласованной с лицензиаром; 2) наличие положительного заключения лицензиара по итогам проведения научно-технической экспертизы опытного образца специального технического средства, предназначенного для проведения оперативно-розыскных мероприятий	значительное
8	Передача в постоянное или временное пользование разработанных специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также документации к ним третьим лицам вне зависимости от форм собственности только по согласованию с лицензиаром	грубое
9	Отсутствие разрешения органов национальной безопасности Республики Казахстан на работу со сведениями, составляющими государственные секреты Республики Казахстан, по заявленному виду деятельности	грубое

10	Уведомление лицензиара о заключенных договорах (контрактах) на разработку специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)	грубое
11	Уведомление лицензиара о заключенных договорах (контрактах) на производство специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)	грубое
Подвид деятельности по ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий		
1	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", " Приборостроение", " Электроэнергетика", " Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование	грубое
2	Наличие минимального набора технических средств и контрольно-измерительного оборудования: 1) мультиметр; 2) осциллограф; 3) вольтметр; 4) амперметр; 5) частотомер; 6) генератор сигналов высокочастотный; 7) генератор сигналов низкочастотный;	грубое

	8) источник постоянного тока с регулировкой силы тока и напряжения; 9) источник переменного регулируемого напряжения (автотрансформатор); 10) индикатор поля; 11) паяльная станция	
3	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)	грубое
4	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом	значительное
5	Передача в постоянное или временное пользование реализуемых или ремонтируемых специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также документации к ним третьим лицам, вне зависимости от форм собственности только по согласованию с лицензиаром	грубое
6	Отсутствие разрешения органов национальной безопасности Республики Казахстан на работу со сведениями, составляющими государственные секреты Республики Казахстан, по заявленному виду деятельности	грубое
7	Уведомление лицензиара о заключенных договорах (контрактах) на приобретение специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала	грубое

	выполнения обязательств по договору (контракту) на реализацию специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий	
8	Уведомление лицензиара о заключенных договорах (контрактах) на ремонт специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)	грубое

Приложение 2
к Критериям оценки степени риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке средств криптографической защиты информации

№ п/п	Показатель субъективного критерия	Источник информации по показателю субъективного критерия	Удельный вес по значимости, балл (в сумме не должен превышать 100 баллов), wi	Условия /значения, xi	
				условие 1 / значение	условие 2/ значение
1	2	3	4	5	
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики			Не выявлено	Выявлено

1	Казахстан от 30 января 2015 года № 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	Включение в график проверок на соответствие требованиям	0 %	100 %
2	Факт перерегистрации лицензиата, изменения его наименования и (или) юридического адреса	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено 0 %	Выявлено 100 %
3	Факт реорганизации юридического лица-лицензиата в соответствии с порядком, определенным статьей 34 Закона "О разрешениях и уведомлениях"	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено 0 %	Выявлено 100 %

Приложение 3
к Критериям оценки степени

риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

№ п/п	Показатель субъективного критерия	Источник информации по показателю субъективного критерия	Удельный вес по значимости, балл (в сумме не должен превышать 100 баллов), wi	Условия /значения, xi	
				условие 1 / значение	условие 2/ значение
1	2	3	4	5	
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных			Не выявлено	Выявлено
					100 %

1	технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	Включение в график проверок на соответствие требованиям	0 %	
2	Факт перерегистрации лицензиата, изменения его наименования или юридического адреса	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено	Выявлено
				0 %	100 %
	Факт реорганизации юридического лица-лицензиата в соответствии с порядком, определенным с	Результаты анализа сведений, представляемых	Включение в	Не выявлено	Выявлено
					100 %

3	татьей 34 Закона "О разрешениях и уведомлениях"	государственными органами и организациями	график проверок на соответствие требованиям	0 %	

Приложение 4
к Критериям оценки степени
риска в сферах обеспечения
информационной безопасности
и специальных технических
средств, предназначенных для
проведения оперативно-
розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности

№ п/п	Показатель субъективного критерия	Источник информации по показателю субъективного критерия	Удельный вес по значимости, балл (в сумме не должен превышать 100 баллов), wi	Условия /значения, xi			
				условие 1 /1 значение	условие 2/2 значение	условие 3/3 значение	условие 4/4 значение
1	2	3	4	5			
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности			За один квартал	За два квартала	За три квартала	За четыре квартала

1	Республики Казахстан от 30 января 2015 года № 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	100	25 %	50 %	75 %	100 %
	Факт перерегистрации лицензиата, изменения его наименован	Результаты анализа сведений, представляемых государственными	Включение в график проверок на соответстви	Не выявлено	Выявлено		
					100 %		

2	ия или юридического адреса	органами и организациями	е требования м	0 %			
3	Факт реорганизации и юридического лица-лицензиата в соответствии с порядком, определенным статьей 34 Закона "О разрешениях и уведомлениях"	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено	Выявлено		
				0 %	100 %		

Приложение 5
к Критериям оценки степени риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности

№ п/п	Показатель субъективн	Источник информации по показателю субъективн	Удельный вес по значимости, балл (в сумме не	Условия /значения, xi			

	о г о критерия	о г о критерия	должен превышать 100 баллов), wi	условие 1 /1 значение	условие 2/2 значение	условие 3/3 значение	условие 4/4 значение
1	2	3	4	5			
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприяти			За один квартал 25 %	За два квартала 50 %	За три квартала	За четыре квартала 100 %

	й " (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)					75 %	
1		Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	100				
2	Факт перерегистрации лицензиата, изменения его наименования или юридического адреса	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено	Выявлено		
				0 %	100 %		
	Факт реорганизации			Не выявлено	Выявлено		

3	юридического лица-лицензиата в соответствии с порядком, определенным статьей 34 Закона "О разрешениях и уведомлениях"	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	0 %	100 %		

Приложение 6
к Критериям оценки степени риска в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке и производству специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

№ п/п	Показатель субъективного критерия	Источник информации по показателю субъективного критерия	Удельный вес по значимости, балл (в сумме не должен превышать 100 баллов), wi	Условия /значения, xi	
				условие 1 / значение	условие 2/ значение
1	2	3	4	5	
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года			За одно полугодие	За два полугодия

1	№ 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	100	50 %	100 %
2	Факт перерегистрации лицензиата, изменения его наименования или юридического адреса	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено 0 %	Выявлено 100 %
3	Факт реорганизации юридического лица-лицензиата в соответствии с порядком, определенным статьей 34 Закона "О разрешениях и уведомлениях"	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	Не выявлено 0 %	Выявлено 100 %

Приложение 7
к Критериям оценки степени
риска в сферах обеспечения
информационной безопасности

и специальных технических
средств, предназначенных для
проведения оперативно-
розыскных мероприятий

Перечень
субъективных критериев для определения степени риска по субъективным критериям в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

№ п/п	Показатель субъективного критерия	Источник информации по показателю субъективного критерия	Удельный вес по значимости, балл (в сумме не должен превышать 100 баллов), wi	Условия /значения, xi			
				условие 1 /1 значение	условие 2/2 значение	условие 3/3 значение	условие 4/4 значение
1	2	3	4	5			
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4 "Об утверждении квалификационных требований и перечня документов, подтверждающих	Результаты мониторинг		За один квартал	За два квартала	За три квартала	За четыре квартала

1	соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	а отчетности и сведений, представляемых субъектом контроля	100	25 %	50 %	75 %	100 %
	Непредставление отчета деятельности, предусмотренного приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4 "Об утверждении квалификац			Не выявлено	Выявлено		

2	ионных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 10473)	Результаты мониторинга отчетности и сведений, представляемых субъектом контроля	Включение в график проверок на соответствие требованиям	0 %	100 %		
3	Факт перерегистрации лицензиата, изменения его наименования или юридического адреса	Результаты анализа сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	0	Факт		
				0 %	100 %		
	Факт реорганизации юридического лица-лиценз	Результаты анализа		Не выявлено	Выявлено		

4	иата в соответствии с порядком, определенным статьей 34 Закона "О разрешениях и уведомлениях"	сведений, представляемых государственными органами и организациями	Включение в график проверок на соответствие требованиям	0 %	100 %		

Приложение 2
к совместному приказу

Приложение 2
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной
экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке средств криптографической защиты информации

Государственный орган, назначивший проверку

_____

Акт о назначении проверки

_____

(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта
(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
	Наличие специалиста, имеющего высшее образование по		

1.	специальности "Математика", "Физика", "Информатика", "Автоматизация и управление", "Информационные системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", "Приборостроение", "Электроэнергетика", "Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", "Системы информационной безопасности", или специалиста, имеющего аналогичное зарубежное высшее образование		
2.	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)		
3.	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом		
	Уведомление лицензиара о заключенных договорах (контрактах) на		

4.	разработку средств криптографической защиты информации не менее чем за пять рабочих дней до начала выполнения обязательств		
5.	Уведомление лицензиара о самостоятельно (за счет собственных средств) разработанных средств криптографической защиты информации не более чем за пять рабочих дней после разработки		

Должностное(-ые) лицо(-а) _____ _____
(должность) (подпись)
_____
(фамилия, имя, отчество (при его наличии)
Руководитель субъекта контроля _____ _____
(должность) (подпись)
_____
(фамилия, имя, отчество (при его наличии)

Приложение 3
к совместному приказу

Приложение 3
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной
экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Государственный орган, назначивший проверку
_____
Акт о назначении проверки
_____
(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта
(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
1.	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", "Приборостроение", "Электроэнергетика", "Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование		
2.	Наличие минимального набора поисковых технических средств: 1) нелинейный локатор (детектор нелинейных переходов); 2) многофункциональный поисковый прибор; 3) мобильный/стационарный комплекс радиомониторинга или сканирующее радиоприемное устройство;		

	4) радиопеленгатор носимый; 5) обнаружитель скрытых видеокамер; 6) стетоскоп; 7) досмотровый комплект зеркал или эндоскоп; 8) анализатор проводных линий; 9) тепловизор		
3.	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)		
4.	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом		
5.	Наличие разработанной и утвержденной лицензиатом по согласованию с лицензиаром: 1) методики проведения работ по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в помещениях и технических средствах;		

	2) методики оценки эффективности защищенности помещений и технических средств от утечки информации по техническим каналам		
6.	Передача в постоянное или временное пользование поисковых технических средств третьим лицам только по согласованию с лицензиаром		
7.	Передача в постоянное или временное пользование разработанной методики третьим лицам только по согласованию с лицензиаром		
8.	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ		
9.	Уведомление лицензиара о выявленных в ходе оказания услуг специальных технических средствах, предназначенных для проведения оперативно-розыскных мероприятий, в течение трех рабочих дней после факта выявления		

Должностное(-ые) лицо(-а) _____ _____

(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)
Руководитель субъекта контроля _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)

Приложение 4
к совместному приказу
Приложение 4
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72 и
Министра национальной
экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по разработке и производству специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Государственный орган, назначивший проверку

_____

Акт о назначении проверки

_____

(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта
(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные		

1.	системы", "Вычислительная техника и программное обеспечение", "Математическое и компьютерное моделирование", "Приборостроение", "Электроэнергетика", "Радиотехника, электроника и телекоммуникации", "Техническая физика", "Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование		
2.	Наличие минимального набора технических средств и контрольно-измерительного оборудования: 1) мультиметр; 2) осциллограф; 3) вольтметр; 4) амперметр; 5) частотомер; 6) генератор сигналов высокочастотный; 7) генератор сигналов низкочастотный; 8) источник постоянного тока с регулировкой силы тока и напряжения; 9) источник переменного регулируемого напряжения (автотрансформатор); 10) индикатор поля; 11) паяльная станция		
3.	Наличие специально выделенного производственного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)		
	Наличие специально выделенного помещения		

4.	для хранения разрабатываемых и произведенных специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий (на праве собственности или ином законном основании)		
5.	Оборудование помещений: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах); 2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом		
6.	Осуществление разработки специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, на условиях: 1) наличия технического задания на разработку специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, утвержденного органом, осуществляющим оперативно-розыскную деятельность, и согласованного с лицензиаром; 2) предоставление лицензиару опытного образца разработанного		

	специального технического средства, предназначенного для проведения оперативно-розыскных мероприятий, для проведения его научно-технической экспертизы		
7.	Осуществление производства специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, на условиях: 1) наличия конструкторской документации на производимое специальное техническое средство, предназначенное для проведения оперативно-розыскных мероприятий, утвержденной органом, осуществляющим оперативно-розыскную деятельность, и согласованной с лицензиаром; 2) наличие положительного заключения лицензиара по итогам проведения научно-технической экспертизы опытного образца специального технического средства, предназначенного для проведения оперативно-розыскных мероприятий		
	Передача в постоянное или временное пользование разработанных специальных технических средств, предназначенных для		

8.	проведения оперативно-розыскных мероприятий, а также документации к ним третьим лицам, вне зависимости от форм собственности только по согласованию с лицензиаром		
9.	Отсутствие разрешения органов национальной безопасности Республики Казахстан на работу со сведениями, составляющими государственные секреты Республики Казахстан, по заявленному виду деятельности		
10.	Уведомление лицензиара о заключенных договорах (контрактах) на разработку специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)		
11.	Уведомление лицензиара о заключенных договорах (контрактах) на производство специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)		

Должностное(-ые) лицо(-а) _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)

Руководитель субъекта контроля _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)

Приложение 5
к совместному приказу
Приложение 5
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной
экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по ремонту и реализации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

Государственный орган, назначивший проверку

_____

Акт о назначении проверки

_____

(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта
(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
	Наличие специалиста, имеющего высшее образование по специальности "Автоматизация и управление", "Информационные системы", "Вычислительная техника и программное		

1.	обеспечение", " Математическое и компьютерное моделирование", " Приборостроение", " Электроэнергетика", " Радиотехника, электроника и телекоммуникации", " Техническая физика", " Космическая техника и технологии", или специалиста, имеющего аналогичное зарубежное высшее образование		
2.	Наличие минимального набора технических средств и контрольно-измерительного оборудования: 1) мультиметр; 2) осциллограф; 3) вольтметр; 4) амперметр; 5) частотомер; 6) генератор сигналов высокочастотный; 7) генератор сигналов низкочастотный; 8) источник постоянного тока с регулировкой силы тока и напряжения; 9) источник переменного регулируемого напряжения (автотрансформатор); 10) индикатор поля; 11) паяльная станция		
3.	Наличие специально выделенного помещения для осуществления заявленного вида деятельности (на праве собственности или ином законном основании)		
	Оборудование помещения: 1) металлическими решетками на окнах (в случае, если помещение находится на первом или последнем этажах);		

4.	2) автоматическими системами охранной и пожарной сигнализации; 3) металлическими опечатываемыми дверями с запирающим устройством; 4) не менее одним опечатываемым металлическим шкафом		
5.	Передача в постоянное или временное пользование реализуемых или ремонтируемых специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также документации к ним третьим лицам, вне зависимости от форм собственности только по согласованию с лицензиаром		
6.	Отсутствие разрешения органов национальной безопасности Республики Казахстан на работу со сведениями, составляющими государственные секреты Республики Казахстан, по заявленному виду деятельности		
7.	Уведомление лицензиара о заключенных договорах (контрактах) на приобретение специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту) на реализацию специальных технических средств,		

	предназначенных для проведения оперативно-розыскных мероприятий		
8.	Уведомление лицензиара о заключенных договорах (контрактах) на ремонт специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, не менее чем за пять рабочих дней до начала выполнения обязательств по договору (контракту)		

Должностное(-ые) лицо(-а) _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)

Руководитель субъекта контроля _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)

Приложение 6
к совместному приказу

Приложение 6
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной
экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности

Государственный орган, назначивший проверку

_____

Акт о назначении проверки

_____

(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта

(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
1.	Наличие специалистов, имеющих высшее или профессиональное техническое образование, прошедших переподготовку, повышение квалификации по направлениям информационной безопасности: 1) не менее трех специалистов, имеющих дипломы о высшем и (или) профессиональном техническом образовании по профилю информационной безопасности (защите информации); 2) не менее двух специалистов, имеющих сертификаты по направлению аудита требованиям международного стандарта ISO 27001; 3) не менее одного специалиста по направлению компьютерной криминалистики (например, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst и другие); 4) не менее одного специалиста по		

	направлению реверс-инжиниринга и (или) анализа вредоносных программ (например, GIAC Reverse Engineering Malware и другие); 5) не менее одного специалиста по направлению этичного хакинга и (или) тестирования на проникновение (например, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester и другие); 6) не менее двух специалистов по направлению администрирования серверных операционных систем (например, Red Hat Certified System Administrator, Microsoft Certified Solutions Associate и другие)			
2.	Наличие минимального набора поисковых средств: 1) решение класса next-generation firewall или unified threat management; 2) система обнаружения угроз на рабочих станциях и реагирования на них (Endpoint Threat Detection and Response); 3) средство проактивного поиска и обнаружения угроз (Threat Hunting); 4) средство предотвращения утечки информации (DLP); 5) система управления событиями информационной безопасности (SIEM);			

	6) платформа реагирования на инциденты (IRP); 7) платформа управления информацией об угрозах (Threat Intelligence Platform); 8) средство динамического анализа вредоносных программ типа "песочница"; 9) сетевой сканер; 10) сканер уязвимостей; 11) сканер уязвимостей веб-приложений; 12) средство эксплуатации уязвимостей; 13) внешний Wi-Fi адаптер с направленной антенной		
3.	Специально выделенное помещение (на праве собственности или иного законного основания)		
4.	Оборудование помещения автоматическими системами охранной и пожарной сигнализации		
5.	Осуществление деятельности при условии: 1) наличия разработанной и утвержденной лицензиатом по согласованию с лицензиаром методики оказания услуг по выявлению технических каналов утечки информации и специальных технических средств оперативным центром информационной безопасности; 2) осуществление заявленного вида деятельности в полном соответствии с методикой оказания		

	услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, оперативным центром информационной безопасности		
6.	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, оперативным центром информационной безопасности (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ		

Должностное(-ые) лицо(-а) _____ _____
(должность) (подпись)

_____

(фамилия, имя, отчество (при его наличии)

Руководитель субъекта контроля _____ _____
(должность) (подпись)

_____

(фамилия, имя, отчество (при его наличии)

Приложение 7
к совместному приказу

Приложение 7
к совместному приказу
Председателя Комитета
национальной безопасности
Республики Казахстан
от 25 октября 2016 года № 72
и Министра национальной

экономики Республики Казахстан
от 9 ноября 2016 года № 471

Проверочный лист
в области разрешительного контроля (в соответствии со статьей 138 Предпринимательского кодекса Республики Казахстан) в отношении субъектов (объектов) контроля, осуществляющих деятельность по оказанию услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности службы реагирования на инциденты информационной безопасности

Государственный орган, назначивший проверку

_____

Акт о назначении проверки

_____

(№, дата)

Наименование субъекта (объекта) контроля

_____

Индивидуальный идентификационный номер/бизнес-идентификационный номер субъекта
(объекта) контроля _____

Адрес места нахождения _____

№	Перечень требований	Соответствует требованиям	Не соответствует требованиям
1	2	3	4
	Наличие специалистов, имеющих высшее или профессиональное техническое образование, прошедших переподготовку, повышение квалификации по направлениям информационной безопасности: 1) не менее трех специалистов, имеющих дипломы о высшем и (или) профессиональном техническом образовании по профилю информационной безопасности (защите информации); 2) не менее двух специалистов, имеющих		

1.	сертификаты по направлению аудита требованиям международного стандарта ISO 27001; 3) не менее одного специалиста по направлению компьютерной криминалистики (например, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst и другие); 4) не менее одного специалиста по направлению реверс-инжиниринга и (или) анализа вредоносных программ (например, GIAC Reverse Engineering Malware и другие); 5) не менее одного специалиста по направлению этичного хакинга и (или) тестирования на проникновение (например, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester и другие)		
2.	Наличие минимального набора поисковых средств: 1) платформа реагирования на инциденты (IRP); 2) платформа управления информацией об угрозах (Threat Intelligence Platform); 3) Средство статического анализа вредоносных программ; 4) Средство динамического анализа вредоносных программ типа "песочница"		

3.	Специально выделенное помещение (на праве собственности или иного законного основания)		
4.	Оборудование помещения автоматическими системами охранной и пожарной сигнализации		
5.	Осуществление деятельности при условии: 1) наличие разработанной и утвержденной лицензиатом по согласованию с лицензиаром методики оказания услуг по выявлению технических каналов утечки информации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности; 2) осуществление заявленного вида деятельности в полном соответствии с методикой оказания услуг по выявлению технических каналов утечки информации специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности		
	Уведомление лицензиара о заключенных договорах (контрактах) на оказание услуг по выявлению		

6.	технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, службой реагирования на инциденты информационной безопасности (в том числе в целях обеспечения собственных нужд лицензиата) не менее чем за пять рабочих дней до начала выполнения работ		

Должностное(-ые) лицо(-а) _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)
Руководитель субъекта контроля _____ _____
(должность) (подпись)

_____
(фамилия, имя, отчество (при его наличии)