

О внесении изменений и дополнения в совместный приказ Заместителя Премьер – Министра Республики Казахстан – Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года № 12 "Об утверждении критериев оценки степени риска и проверочных листов в сфере информатизации в части обеспечения информационной безопасности"

Совместный приказ и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 10 сентября 2026 года № 550/НҚ и Заместителя Премьер-Министра – Министра национальной экономики Республики Казахстан от 11 сентября 2026 года № 145. Зарегистрирован в Министерстве юстиции Республики Казахстан 18 сентября 2026 года № 39905

ПРИКАЗЫВАЕМ:

1. Внести в совместный приказ Заместителя Премьер – Министра Республики Казахстан – Министра оборонной и аэрокосмической промышленности Республики Казахстан от 29 января 2019 года № 13/НҚ и Министра национальной экономики Республики Казахстан от 29 января 2019 года №12 "Об утверждении критериев оценки степени риска и проверочных листов в сфере информатизации в части обеспечения информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов № 18269) следующие изменения и дополнение:

в пункте 1:

подпункт 3) изложить в следующей редакции:

"3) критерии оценки степени риска в сфере цифровизации в части кибербезопасности, согласно приложению 3 к настоящему совместному приказу.";

дополнить подпунктом 4) следующего содержания:

"4) проверочный лист в сфере цифровизации в части кибербезопасности в отношении государственных юридических лиц, субъектов квазигосударственного сектора, собственников и владельцев негосударственных цифровых систем, интегрируемых с цифровыми системами государственных органов или предназначенных для формирования государственных цифровых ресурсов, центров обеспечения кибербезопасности, а также собственников и владельцев критически важных цифровых объектов согласно приложению 4 к настоящему совместному приказу.";

приложение 3 изложить в новой редакции согласно приложению 1 к настоящему приказу;

дополнить приложением 4 согласно приложению 2 к настоящему приказу.

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития 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 Министерства искусственного интеллекта и цифрового развития Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего совместного приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства искусственного интеллекта и цифрового развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта;

4) в течение пяти рабочих дней после государственной регистрации настоящего совместного приказа в Министерстве юстиции Республики Казахстан его направление в Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан для размещения в информационной системе "Единый реестр субъектов и объектов проверок".

4. Контроль за исполнением настоящего совместного приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

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

Заместитель Премьер-Министра –
Министр национальной экономики
Республики Казахстан

Исполняющий обязанности министра
искусственного интеллекта и цифрового развития
Республики Казахстан _____ С. Жумангарин

"СОГЛАСОВАН"

Генеральная прокуратура
Республики Казахстан

"СОГЛАСОВАН"

Комитет национальной безопасности
Республики Казахстан

Приложение 1
к совместному приказу
Заместитель Премьер-Министра

—

Министр национальной
экономики
Республики Казахстан

от 11 сентября 2026 года № 145
и Исполняющий обязанности
министра искусственного
интеллекта и цифрового
развития Республики Казахстан
от 10 сентября 2026 года
№ 550/НК

Приложение 3
к совместному приказу
Заместителя Премьер-Министра
Республики Казахстан –
Министра
оборонной и аэрокосмической
промышленности
Республики Казахстан
от 29 января 2019 года № 13/НК
и Министра национальной
экономики Республики
Казахстан
от 29 января 2019 года
№ 12

Критерии оценки степени риска в сфере цифровизации в части кибербезопасности

Глава 1. Общие положения

1. Настоящие Критерии оценки степени риска в сфере цифровизации в части кибербезопасности (далее – Критерии) разработаны в соответствии с пунктами 5 и 6 статьи 141, статьи 143 Предпринимательского кодекса Республики Казахстан (далее – Кодекс), приказом исполняющего обязанности Министра национальной экономики Республики Казахстан от 22 июня 2022 года № 48 "Об утверждении Правил формирования регулируемыми государственными органами системы оценки и управления рисками и о внесении изменений в приказ исполняющего обязанности Министра национальной экономики Республики Казахстан от 31 июля 2018 года № 3 "Об утверждении Правил формирования государственными органами системы оценки рисков и формы проверочных листов" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 31148) и формой проверочного листа, утвержденной приказом исполняющего обязанности Министра национальной экономики Республики Казахстан от 31 июля 2018 года № 3 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 17371).

2. В настоящих критериях используются следующие понятия:

1) грубое нарушение – не соблюдение требований нормативных правовых актов Республики Казахстан в сфере цифровизации в части кибербезопасности приведшее

или которое может привести к невозможности предоставления услуг, значительным негативным последствиям для цифровых ресурсов, цифровых систем и других цифровых объектов;

2) значительное нарушение – не соблюдение требований нормативных правовых актов Республики Казахстан в сфере цифровизации в части кибербезопасности, приведшее или которое может привести к существенному ограничению предоставления услуг, существенному ухудшению ситуации или существенным негативным последствиям для цифровых ресурсов, цифровых систем и других цифровых объектов, наличие двух или более подтвержденных жалоб или обращений в сфере цифровизации в части кибербезопасности;

3) незначительное нарушение – не соблюдение требований нормативных правовых актов Республики Казахстан в сфере цифровизации в части кибербезопасности, приведшее или которое может привести к несущественным инцидентам, не оказывающим влияние на цифровые ресурсы, цифровые системы и другие цифровые объекты;

4) 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;

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

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

7) 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 профилактического контроля с посещением субъекта (объекта) контроля 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 профилактического контроля с посещением субъекта (объекта) контроля;

8) субъекты контроля в сфере цифровизации в части кибербезопасности (далее – субъекты контроля) – субъекты квазигосударственного сектора, собственники и владельцы негосударственных цифровых систем, интегрируемых с цифровыми системами государственных органов или предназначенных для формирования

государственных цифровых ресурсов, центры обеспечения кибербезопасности, а также собственники и владельцы критически важных цифровых объектов;

9) 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.

3. Критерии оценки степени риска для профилактического контроля с посещением субъекта (объекта) контроля формируются посредством объективных и субъективных критериев.

Глава 2. Объективные критерии

4. На первом этапе по объективным критериям субъекты контроля распределяются по трем степеням риска: высокая, средняя и низкая.

5. К субъектам высокой степени риска относятся собственники и владельцы критических важных цифровых объектов.

К субъектам средней степени риска относятся субъекты квазигосударственного сектора и собственники и владельцы негосударственных цифровых систем, интегрируемых с цифровыми системами государственных органов или предназначенных для формирования государственных цифровых ресурсов.

К субъектам низкой степени риска относятся центры обеспечения кибербезопасности.

Глава 3. Субъективные критерии

6. Субъективные критерии разработаны на основании требований, перечисленных в проверочных листах (далее – требования) несоблюдение которых в соответствии с критериями оценки степени риска соответствуют определенной степени нарушения. В отношении каждого требования из проверочных листов определяется степень нарушения согласно приложению к настоящим критериям.

7. Определение субъективных критериев осуществляется с применением следующих этапов:

- 1) формирование базы данных и сбор информации;
- 2) анализ информации и оценка рисков.

8. Формирование базы данных и сбор информации необходимы для выявления субъектов (объектов) контроля, нарушающих законодательство Республики Казахстан в сфере цифровизации в части кибербезопасности.

9. Для оценки степени рисков по субъективным критериям используются результаты предыдущего профилактического контроля с посещением субъектов (объектов) контроля и проверки;

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

Одно невыполненное требование грубой степени приравнивается к показателю 100 и это является основанием для проведения профилактического контроля с посещением субъекта (объекта) контроля.

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

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

$$SP3 = (SP2 \times 100 / SP1) \times 0,7, \text{ где:}$$

SP3 - 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:

$$SPH = (SP2 \times 100 / SP1) \times 0,3, \text{ где:}$$

SPH - 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:

$$SP = SP3 + SPH \text{ где:}$$

SP - показатель степени риска по нарушениям;

SP3 - показатель значительных нарушений;

SPH - показатель незначительных нарушений.

По показателям степени риска субъект контроля относится:

к высокой степени риска – при показателе степени риска от 71 до 100 включительно и в отношении него проводится профилактический контроль с посещением субъекта контроля;

не отнесенной к высокой степени риска – при показателе степени риска от 0 до 71 включительно и в отношении него не проводится профилактический контроль с посещением субъекта контроля.

11. Кратность проведения профилактического контроля с посещением субъекта (объекта) контроля составляет не чаще одного раза в полугодие.

12. Профилактический контроль с посещением субъекта контроля проводятся на основании полугодовых списков профилактического контроля с посещением субъекта контроля.

13. Списки профилактического контроля с посещением субъекта контроля составляются с учетом приоритетности субъектов контроля с наибольшим показателем степени риска по субъективным критериям.

Приложение
к Критериям оценки
степени риска в
сфере цифровизации в части
кибербезопасности

Перечень субъективных критериев для определения степени риска по субъективным критериям

№	Критерии	Степень нарушения
Результаты предыдущих проверок и профилактического контроля с посещением (степень тяжести устанавливается при несоблюдении нижеперечисленных требований)		
1.	Соблюдение требований по осуществлению подключения локальных, ведомственных и корпоративных сетей телекоммуникаций государственных органов, местных исполнительных органов (далее-МИО), государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцев критически важные цифровые объекты (далее-КВЦО), за исключением банков второго уровня и объектов среднего образования сельских населенных пунктов, использующих спутниковые (космические) каналы связи для доступа к Интернету, операторами связи через единый шлюз доступа к Интернету	Значительное
2.	Соблюдение требований по оповещению владельцем критически важных цифровых объектов Национального координационного центра кибербезопасности об инцидентах кибербезопасности	Грубое
	Соблюдение требований по применению средств: идентификации, аутентификации и управления доступом пользователей; идентификации оборудования; защиты диагностических и конфигурационных портов;	

3.	физического сегментирования локальной сети; логического сегментирования локальной сети; управления сетевыми соединениями; межсетевого экранирования; сокрытия внутреннего адресного пространства локальной сети; контроля целостности данных, сообщений и конфигураций; криптографической защиты информации	Значительное
4.	Соблюдение требований по подключению к системе мониторинга обеспечения кибербезопасности, защиты и безопасного функционирования при эксплуатации цифровых объектов "цифрового правительства" первого и второго классов в соответствии с классификатором	Значительное
5.	Соблюдение требований по наличию антивирусных средств, обновлений операционных систем на рабочих станциях, подключенных к сети Интернет при организации доступа к Интернету из локальных сетей внешнего контура	Значительное
6.	Соблюдение требования по наличию подразделения кибербезопасности, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов, или определение должностного лица, ответственного за обеспечение кибербезопасности, с прохождением специализированных курсов в сфере обеспечения кибербезопасности не реже одного раза в три года с выдачей сертификата	Грубое
	Соблюдение требования по наличию и соответствию нормативно-технической документации (далее – ТД) по	

обеспечению кибербезопасности, в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется государственные органы (далее-ГО), МИО или организация в своей деятельности.

ТД по обеспечению кибербезопасности разрабатывается на казахском и русском языках, утверждается правовым актом государственных органов и МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации. ТД по обеспечению кибербезопасности пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.

1. Политика кибербезопасности ГО, МИО или организации является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения кибербезопасности.

2. В перечень документов второго уровня входят документы, детализирующие требования политики кибербезопасности ГО, МИО или организации, в том числе:

- 1) методика оценки рисков кибербезопасности;
- 2) правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;
- 3) правила проведения внутреннего аудита кибербезопасности;
- 4) правила использования средств криптографической защиты информации (далее-СКЗИ);
- 5) правила организации процедуры аутентификации и разграничения прав доступа к цифровым ресурсам;

6) правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;

7) правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

3. Документы третьего уровня содержат описание процессов и процедур обеспечения кибербезопасности, в том числе:

1) каталог угроз (рисков) кибербезопасности;

2) план обработки угроз (рисков) кибербезопасности;

3) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

4) руководство администратора по сопровождению цифрового объекта, резервному копированию и восстановлению информации;

5) инструкцию о порядке действий пользователей по реагированию на инциденты кибербезопасности и во внештатных (кризисных) ситуациях.

4. Перечень документов четвертого уровня включает рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения выполненных процедур и работ, в том числе:

1) журнал регистрации инцидентов кибербезопасности и учета внештатных ситуаций;

2) журнал посещения серверных помещений;

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений;

5) журнал учета резервных копий (резервного копирования,

	восстановления), тестирования резервных копий	
8.	Соблюдение требований при доступе к цифровым объектам первого и второго классов в соответствии с классификатором по применению многофакторной аутентификации, в том числе с использованием цифровых сертификатов	Значительное
9.	Соблюдение требований по внесению в должностные инструкции и функциональные обязанности по обеспечению кибербезопасности и обязательств по исполнению требований ТД по обеспечению кибербезопасности служащих ГО, МИО или работников организации	Значительное
10.	Соблюдение требования по применению СКЗИ для цифровых объектов: первого класса в соответствии с классификатором – третьего уровня безопасности; второго класса в соответствии с классификатором – второго уровня безопасности; третьего класса в соответствии с классификатором – первого уровня безопасности.	Грубое
11.	Соблюдение требований собственником или владельцем объекта цифровой инфраструктуры "цифрового правительства", а также оператором "цифрового правительства" хранение государственных цифровых ресурсов (далее – ЦР), содержащихся в объектах цифровой инфраструктуры "цифрового правительства".	Грубое
	Соблюдение требований для обеспечения кибербезопасности ЦР по применению систем управления содержимым (контентом), выполняющая: санкционирование операций размещения, изменения и удаления в ЦР;	

12.	регистрацию авторства при размещении, изменении и удалении ЦР; проверку загружаемого ЦР на наличие вредоносного кода; аудит безопасности исполняемого кода и скриптов; контроль целостности размещенного ЦР; ведение журнала изменений ЦР; мониторинг аномальной активности пользователей и программных роботов	Грубое
13.	Соблюдение требований по применению регистрационных свидетельств для проверки подлинности доменного имени и криптографической защиты содержимого сеанса связи с использованием СКЗИ для обеспечения кибербезопасности ЦР	Значительное
14.	Соблюдения требований по управлению идентификацией при использовании технологии виртуализации: аутентификация клиентов цифровых услуг и привилегированных пользователей; федеративной идентификации пользователей в пределах одной технологической платформы; сохранения информации об аутентификации после удаления идентификатора пользователя; применения средств контроля процедур назначения профилей полномочий пользователя	Значительное
15.	Соблюдение требований по проведению аудита событий кибербезопасности при использовании технологии виртуализации: обязательность и регулярность процедур, определяемых в ТД по обеспечению кибербезопасности; проведения процедур аудита для всех операционных систем, клиентских виртуальных машин, инфраструктуры сетевых компонентов;	Значительное

	ведения журнала регистрации событий и хранения в недоступной для администратора системе хранения; проверки правильности работы системы ведения журнала регистрации событий; определения длительности хранения журналов регистрации событий в ТД по обеспечению кибербезопасности.	
16.	Соблюдение требований регистрации событий кибербезопасности при использовании технологии виртуализации: журналирования действий администраторов; применения системы мониторинга инцидентов и событий кибербезопасности; оповещения на основе автоматического распознавания критического события или инцидента кибербезопасности.	Значительное
17.	Соблюдение требований по исполнению процедур сетевого и системного администрирования: обеспечения сохранности образов виртуальных машин, контроля целостности операционной системы, приложений, сетевой конфигурации, программных обеспечений (далее – ПО) и данных ГО или организации на наличие вредоносных сигнатур; отделения аппаратной платформы от операционной системы виртуальной машины с целью исключения доступа внешних пользователей к аппаратной части	Значительное
18.	Соблюдение требования по обеспечению системы хранения данных системой резервного копирования.	Значительное
19.	Соблюдение требования по применению программно-технических средств защиты информации, в том числе криптографического шифрования, с использованием СКЗИ при организации выделенного канала	Значительное

	связи, объединяющего локальные сети.	
20.	Соблюдение требования по исключению сопряжения локальной сети (далее – ЛС) внутреннего контура и ЛС внешнего контура цифровые субъекты (далее – ЦС) между собой, за исключением организованных каналов связи с использованием СКЗИ, для учреждений Республики Казахстан, находящихся за границей или организованных с применением экранированной подсети	Грубое
21.	Соблюдение требований по использованию ведомственной электронной почты, службы мгновенных сообщений и иных сервисов; электронной почты, службы мгновенных сообщений и иных сервисов, центры управления и сервера которых физически размещены на территории Республики Казахстан, если иное не установлено уполномоченным органом, для осуществления оперативного информационного обмена в электронной форме служащими ГО, МИО и работниками государственных юридических лиц, субъектами квазигосударственного сектора, а также владельцами критически важных цифровых объектов при исполнении ими служебных обязанностей	Значительное
22.	Соблюдение требования по наличию бесперебойного электропитания для активного оборудования локальных сетей.	Значительное
23.	Соблюдение требования по физическому отключению неиспользуемых портов кабельной системы локальной сети от активного оборудования.	Незначительное
24.	Соблюдение требования по применению межсетевое экранирования.	Значительное

Соблюдение следующих требований по серверному помещению:

1) Наличие документирования при техническом сопровождении оборудования, установленного в серверном помещении: обслуживание оборудования; устранение проблем, возникающих при работе аппаратно-программного обеспечения; факты сбоев и отказов, а также результаты восстановительных работ; послегарантийное обслуживание критически важного оборудования по истечении гарантийного срока обслуживания.

2) Наличие системы контроля и управления доступом обеспечивающие санкционированный вход и санкционированный выход;

3) Наличие в актуальном состоянии списка лиц, авторизованных для осуществления сопровождения объектов цифровой инфраструктуры;

4) Наличие системы обеспечения микроклимата;

5) Наличие системы охранной сигнализации;

6) Наличие системы видеонаблюдения;

7) Наличие системы пожарной сигнализации;

8) Наличие системы пожаротушения;

9) Наличие системы гарантированного электропитания ;

10) Наличие системы заземления;

11) Соблюдение требования по проведению на регулярной основе инвентаризации серверного оборудования с проверкой его конфигурации;

12) Соблюдение требования по размещению серверного оборудования

Грубое

	аппаратно-программного комплекса системы хранения данных в серверном помещении; 13) Соблюдение требования по расположению серверного помещения в отдельных, непроходных помещениях без оконных проемов. В случае наличия оконных проемов, они закрываются или заделываются негорючими материалами. Для поверхности стен, потолков и пола применяются материалы, не выделяющие и не накапливающие пыль; 14) Наличие фальшпола и (или) фальшпотолка для размещения кабельных систем и инженерных коммуникаций; 15) Соблюдение требования по исключению прохождения любых транзитных коммуникаций; 16) Соблюдение требования по расположению основных и резервных серверных помещений на безопасном расстоянии в удаленных друг от друга зданиях. Требования к резервным серверным помещениям идентичны требованиям к основным серверным помещениям.	
26.	Соблюдение следующих требований по кроссовому помещению: 1) Отсутствие мощных источников электромагнитных помех; 2) Отсутствие труб и вентилей системы водоснабжения; 3) Наличие систем пожарной безопасности; 4) Отсутствие легко возгораемых материалов; 5) Наличие отдельной линии электропитания от отдельного автомата для подключения шкафа по проекту; 6) Наличие систем охранной сигнализации, контроля доступа; 7) Наличие системы кондиционирования.	Грубое

27.	Соблюдение требования использования на этапе опытной и промышленной эксплуатации цифровых объектов средств и систем: мониторинга и управления инцидентами и событиями кибербезопасности; цифровой инфраструктурой; обнаружения и предотвращения вторжений.	Значительное
28.	Соблюдение требования по созданию собственного центра обеспечения кибербезопасности и обеспечению его функционирования или приобретению услуг центра обеспечения кибербезопасности у третьих лиц, а также взаимодействие его с Национальным координационным центром кибербезопасности.	Грубое
29.	Соблюдение требований по размещению на Интернет-ресурсе с зарегистрированным доменным именем .KZ и (или) .ҚАЗ на аппаратно-программном комплексе, который расположен на территории Республики Казахстан. использованию доменных имен .KZ и (или) .ҚАЗ в пространстве казахстанского сегмента Интернета при передаче данных интернет-ресурсами с применением сертификатов безопасности.	Значительное
30.	Соблюдение ГО, МИО и организацией требования по приобретению товаров в целях реализации требований обеспечения кибербезопасности для обороны страны и безопасности государства из реестра доверенного программного обеспечения и продукции электронной промышленности.	Незначительное
	Соблюдение требований по контролю событий нарушений кибербезопасности в ГО, МИО или организации: 1) проведение мониторинга событий, связанных с нарушением	

31.

кибербезопасности, и анализ результатов мониторинга;

2) регистрация события, связанные с состоянием кибербезопасности, и выявляются нарушения путем анализа журналов событий, в том числе: журналов событий операционных систем; журналов событий систем управления базами данных; журналов событий антивирусной защиты; журналов событий прикладного ПО; журналов событий телекоммуникационного оборудования; журналов событий систем обнаружения и предотвращения атак; журналов событий системы управления контентом;

3) обеспечение синхронизации времени журналов регистрации событий с инфраструктурой источника времени;

4) хранение журналов регистрации событий в течение срока, указанного в ТД по обеспечению кибербезопасности, но не менее трех лет и нахождения в оперативном доступе не менее двух месяцев;

5) ведение журналов регистрации событий;

6) обеспечение защиты журналов регистрации событий от вмешательства и неавторизованного доступа. Не допущение наличие у системных администраторов полномочий на изменение, удаление и отключение журналов. Для конфиденциальных ЦС требуются создание и ведение резервного хранилища журналов;

7) обеспечение внедрения формализованной процедуры информирования об инцидентах кибербезопасности и реагирования на инциденты кибербезопасности.

Значительное

32.	Соблюдение требования по наличию соглашения, в котором устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение при привлечении сторонних организаций к обеспечению кибербезопасности ЦР, ЦС, цифровой инфраструктуры.	Грубое
33.	Соблюдение требований при внесении изменений в условия трудового договора работника организации, ротации или продвижении по государственной службе служащего ГО, МИО, их увольнении права доступа к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего служащего ГО, МИО или работника организации, аннулируются.	Грубое
34.	Соблюдение требования организации и ведения учета прохождения служащими ГО, МИО или работниками организаций повышения обучения в сфере цифровизации и области обеспечения кибербезопасности с выдачей электронного сертификата, обеспечением хранения в материалах личного дела кадровой службой.	Незначительное
35.	Соблюдение требований по регистрации в службе реагирования на компьютерные инциденты государственной технической службы, события кибербезопасности идентифицированных как критические для конфиденциальности, доступности и целостности по результатам анализа мониторинга событий кибербезопасности и анализа журнала событий.	Значительное
	Соблюдение требования по проведению аудита	

36.	кибербезопасности не реже одного раза в год, владельцам критически важных цифровых объектов, обрабатывающих данные, содержащие охраняемую законом тайну.	Значительное
37.	Соблюдение требования по наличию протоколов с положительным результатом испытаний на соответствие требованиям кибербезопасности.	Значительное
38.	Соблюдение требований по обеспечению разрабатываемого или приобретаемого готового прикладного ПО интерфейсом пользователя, ввод, обработку и вывод данных на казахском, русском и других языках, по необходимости, с возможностью выбора пользователем языка интерфейса.	Незначительное
39.	Соблюдение требований по осуществлению мониторинга: действий пользователей и персонала; использования средств обработки информации.	Незначительное
40.	Соблюдение требования по обеспечению разрабатываемого или приобретаемого готового прикладного ПО технической документацией по эксплуатации на казахском и русском языках.	Незначительное
41.	Соблюдение требований по обеспечению высокой доступности сервера встроенных систем: 1) горячей замены резервных вентиляторов, блоков питания, дисков и адаптеров ввода-вывода; 2) оповещения о критических событиях; 3) поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.	Значительное
42.	Соблюдение требований по наличию программного и аппаратного обеспечения гарантированного уничтожения информации при выводе из эксплуатации носителей	Значительное

	информации, используемых в конфиденциальных ЦС, конфиденциальных ЦР и ЦР, содержащих персональные данные ограниченного доступа.	
43.	Соблюдение требования по наличию документированной схемы локальной сети, которая поддерживается в актуальном состоянии при эксплуатации.	Незначительное
44.	Соблюдение требований по применению системы предотвращения утечки данных (DLP) для защиты цифровых объектов ГО, МИО и критически важных цифровых объектов При этом обеспечиваются: визуальное уведомление пользователя о проводимом контроле действий; размещение центра управления и серверов системы предотвращения утечки данных в пределах локальной сети.	Незначительное
45.	Соблюдение требований по интеграции ЦС ГО или МИО, в том числе с ЦС ГО и МИО, находящейся в опытной эксплуатации.	Значительное
46.	Соблюдение требований по не допущению подключения к единой транспортной среде государственных органов (далее - ЕТС ГО), локальной сети цифровых субъектов, а также техническим средствам, входящим в состав ЕТС ГО, локальной сети цифровых субъектов, устройств для организации удаленного доступа посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи, абонентских устройств сотовой связи и других беспроводных сетевых устройств, за исключением организованных оператором "цифрового правительства" беспроводных каналов связи ЕТС ГО, с использованием СКЗИ.	Грубое

47.	Соблюдение требования по вводу в промышленную эксплуатацию цифрового объекта "цифрового правительства" осуществляется его собственником или владельцем только с использованием исполняемых кодов, скомпонованных из исходных кодов цифровых объектов "цифрового правительства", переданных ему государственной технической службой.	Значительное
48.	Соблюдение требования по исключению подключения ЛС внутреннего контура цифровых субъектов к Интернету.	Грубое
49.	Соблюдение требования по обеспечению собственником и (или) владельцем ЦР создания общедоступных ЦР на казахском, русском и, по необходимости, на других языках, с возможностью выбора пользователем языка интерфейса.	Незначительное
50.	Соблюдение требований по вводу в промышленную эксплуатацию ЦС ГО, МИО и организаций в соответствии с требованиями технической документации при условии положительного завершения опытной эксплуатации, наличия протоколов испытаний с положительными результатами испытаний на соответствие требованиям кибербезопасности, подписания акта о вводе в промышленную эксплуатацию ЦС приемочной комиссией с участием представителей уполномоченных органов в сферах цифровизации и обеспечения кибербезопасности, заинтересованных ГО, МИО и организаций.	Значительное

Приложение 2
к совместному приказу
Заместитель Премьер-
Министра – Министр
национальной экономики
Республики Казахстан
от 11 сентября 2026 года
№ 145 и

Исполняющий обязанности
министра искусственного
интеллекта и цифрового
развития Республики Казахстан
от 10 сентября 2026 года
№ 550/НК

Приложение 4
к совместному приказу
Заместителя Премьер-
Министра Республики Казахстан

—
Министра оборонной и
аэрокосмической
промышленности
Республики Казахстан
от 29 января 2019 года
№13/НК

и Министра национальной
экономики
Республики Казахстан
от 29 января 2019 года
№12

**Проверочный лист в сфере цифровизации в части кибербезопасности в соответствии со
статьей 138 Предпринимательского кодекса Республики Казахстан в отношении субъектов
квазигосударственного сектора, собственников и владельцев негосударственных цифровых
систем, интегрируемых с цифровыми системами государственных органов или
предназначенных для формирования государственных цифровых ресурсов, центров
обеспечения кибербезопасности, а также собственников и владельцев критически важных
цифровых объектов**

наименование однородной группы субъектов (объектов) контроля

Государственный орган, назначивший проверку/профилактического контроля с
посещением субъекта (объекта) контроля

Акт о назначении проверки/профилактического контроля с посещением субъекта
объекта) контроля _____

№, 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	Соблюдение требований по осуществлению подключения локальных, ведомственных и корпоративных сетей телекоммуникаций государственных органов, местных исполнительных органов (далее-МИО), государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцев критически важные цифровые объекты (далее-КВЦО), за исключением банков второго уровня и объектов среднего образования сельских населенных пунктов, использующих спутниковые (космические) каналы связи для доступа к Интернету, операторами связи через единый шлюз доступа к Интернету		
2	Соблюдение требований по оповещению владельцем критически важных цифровых объектов Национального координационного центра кибербезопасности об инцидентах кибербезопасности		
	Соблюдение требований по применению средств: идентификации, аутентификации и управления доступом пользователей;		

3	идентификации оборудования; защиты диагностических и конфигурационных портов; физического сегментирования локальной сети; логического сегментирования локальной сети; управления сетевыми соединениями; межсетевого экранирования; сокрытия внутреннего адресного пространства локальной сети; контроля целостности данных, сообщений и конфигураций; криптографической защиты информации		
4	Соблюдение требований по подключению к системе мониторинга обеспечения кибербезопасности, защиты и безопасного функционирования при эксплуатации цифровых объектов "цифрового правительства" первого и второго классов в соответствии с классификатором		
5	Соблюдение требований по наличию антивирусных средств, обновлений операционных систем на рабочих станциях, подключенных к сети Интернет при организации доступа к Интернету из локальных сетей внешнего контура		
	Соблюдение требования по наличию подразделения кибербезопасности, являющееся структурным подразделением,		

6	обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов, или определение должностного лица, ответственного за обеспечение кибербезопасности, с прохождением специализированных курсов в сфере обеспечения кибербезопасности не реже одного раза в три года с выдачей сертификата		
	Соблюдение требования по наличию и соответствию нормативно-технической документации (далее – ТД) по обеспечению кибербезопасности, в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется государственные органы (далее-ГО), МИО или организация в своей деятельности. ТД по обеспечению кибербезопасности разрабатывается на казахском и русском языках, утверждается правовым актом государственных органов и МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации. ТД по обеспечению кибербезопасности		

пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.

1. Политика кибербезопасности ГО, МИО или организации является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения кибербезопасности.

2. В перечень документов второго уровня входят документы, детализирующие требования политики кибербезопасности ГО, МИО или организации, в том числе:

- 1) методика оценки рисков кибербезопасности;
- 2) правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;
- 3) правила проведения внутреннего аудита кибербезопасности;
- 4) правила использования средств криптографической защиты информации (далее-СКЗИ);
- 5) правила организации процедуры аутентификации и разграничения прав доступа к цифровым ресурсам;
- 6) правила организации антивирусного контроля, использования мобильных устройств, носителей информации,

Интернета и электронной почты;

7) правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации.

3. Документы третьего уровня содержат описание процессов и процедур обеспечения кибербезопасности, в том числе:

1) каталог угроз (рисков) кибербезопасности;

2) план обработки угроз (рисков) кибербезопасности;

3) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

4) руководство администратора по сопровождению цифрового объекта, резервному копированию и восстановлению информации;

5) инструкцию о порядке действий пользователей по реагированию на инциденты кибербезопасности и во внештатных (кризисных) ситуациях.

4. Перечень документов четвертого уровня включает рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения

	выполненных процедур и работ, в том числе: 1) журнал регистрации инцидентов кибербезопасности и учета внештатных ситуаций; 2) журнал посещения серверных помещений; 3) отчет о проведении оценки уязвимости сетевых ресурсов; 4) журнал учета кабельных соединений; 5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий		
8	Соблюдение требований при доступе к цифровым объектам первого и второго классов в соответствии с классификатором по применению многофакторной аутентификации, в том числе с использованием цифровых сертификатов		
9	Соблюдение требований по внесению в должностные инструкции и функциональные обязанности по обеспечению кибербезопасности и обязательств по исполнению требований ТД по обеспечению кибербезопасности служащих ГО, МИО или работников организации		
	Соблюдение требования по применению СКЗИ для цифровых объектов: первого класса в соответствии с классификатором – третьего уровня безопасности;		

10	второго класса в соответствии с классификатором – второго уровня безопасности; третьего класса в соответствии с классификатором – первого уровня безопасности.		
11	Соблюдение требований собственником или владельцем объекта цифровой инфраструктуры "цифрового правительства", а также оператором "цифрового правительства" хранение государственных цифровых ресурсов (далее – ЦР), содержащихся в объектах цифровой инфраструктуры "цифрового правительства".		
12	Соблюдение требований для обеспечения кибербезопасности ЦР по применению систем управления содержимым (контентом), выполняющая: санкционирование операций размещения, изменения и удаления в ЦР; регистрацию авторства при размещении, изменении и удалении ЦР; проверку загружаемого ЦР на наличие вредоносного кода; аудит безопасности исполняемого кода и скриптов; контроль целостности размещенного ЦР; ведение журнала изменений ЦР;		

	мониторинг аномальной активности пользователей и программных роботов		
13	Соблюдение требований по применению регистрационных свидетельств для проверки подлинности доменного имени и криптографической защиты содержимого сеанса связи с использованием СКЗИ для обеспечения кибербезопасности ЦР		
14	Соблюдения требований по управлению идентификацией при использовании технологии виртуализации: аутентификация клиентов цифровых у с л у г и привилегированных пользователей; федеративной идентификации пользователей в пределах одной технологической платформы; сохранения информации об аутентификации после у д а л е н и я идентификатора пользователя; применения средств контроля процедур назначения профилей полномочий пользователя		
	Соблюдение требований по проведению аудита с о б ы т и й кибербезопасности при использовании технологии виртуализации: обязательность и регулярность процедур,		

15	определяемых в ТД по обеспечению кибербезопасности; проведения процедур аудита для всех операционных систем, клиентских виртуальных машин, инфраструктуры сетевых компонентов; ведения журнала регистрации событий и хранения в недоступной для администратора системе хранения; проверки правильности работы системы ведения журнала регистрации событий; определения длительности хранения журналов регистрации событий в ТД по обеспечению кибербезопасности.		
16	Соблюдение требований регистрации событий кибербезопасности при использовании технологии виртуализации: журналирования действий администраторов; применения системы мониторинга инцидентов и событий кибербезопасности; оповещения на основе автоматического распознавания критического события или инцидента кибербезопасности.		
	Соблюдение требований по исполнению процедур сетевого и системного администрирования: обеспечения сохранности образов виртуальных машин, контроля целостности операционной системы, приложений, сетевой		

17	конфигурации, программных обеспечений (далее – ПО) и данных ГО или организации на наличие вредоносных сигнатур; отделения аппаратной платформы от операционной системы виртуальной машины с целью исключения доступа внешних пользователей к аппаратной части		
18	Соблюдение требования по обеспечению системы хранения данных системой резервного копирования.		
19	Соблюдение требования по применению программно-технических средств защиты информации, в том числе криптографического шифрования, с использованием СКЗИ при организации выделенного канала связи, объединяющего локальные сети.		
20	Соблюдение требования по исключению сопряжения локальной сети (далее – ЛС) внутреннего контура и ЛС внешнего контура цифровые субъекты (далее – ЦС) между собой, за исключением организованных каналов связи с использованием СКЗИ, для учреждений Республики Казахстан, находящихся за границей или организованных с применением экранированной подсети		
	Соблюдение требований по использованию ведомственной электронной почты, службы мгновенных		

21	сообщений и иных сервисов; электронной почты, службы мгновенных сообщений и иных сервисов, центры управления и сервера которых физически размещены на территории Республики Казахстан, если иное не установлено уполномоченным органом, для осуществления оперативного информационного обмена в электронной форме служащими ГО, МИО и работниками государственных юридических лиц, субъектами квазигосударственного сектора, а также владельцами критически важных цифровых объектов при исполнении ими служебных обязанностей		
22	Соблюдение требования по наличию бесперебойного электропитания для активного оборудования локальных сетей.		
23	Соблюдение требования по физическому отключению неиспользуемых портов кабельной системы локальной сети от активного оборудования.		
24	Соблюдение требования по применению межсетевого экранирования.		
	Соблюдение следующих требований по серверному помещению: 1) Наличие документирования при техническом		

сопровождении
оборудования,
установленного в
серверном помещении:
обслуживание
оборудования;
устранение проблем,
возникающих при работе
аппаратно-программного
обеспечения; факты
сбоев и отказов, а также
результаты
восстановительных работ
; послегарантийное
обслуживание
критически важного
оборудования по
истечении гарантийного
срока обслуживания.

2) Наличие системы
контроля и управления
д о с т у п о м
обеспечивающие
санкционированный вход
и санкционированный
выход;

3) Наличие в актуальном
состоянии списка лиц,
авторизованных для
осуществления
сопровождения объектов
ц и ф р о в о й
инфраструктуры;

4) Наличие системы
обеспечения
микроклимата;

5) Наличие системы
охранной сигнализации;

6) Наличие системы
видеонаблюдения;

7) Наличие системы
пожарной сигнализации;

8) Наличие системы
пожаротушения;

9) Наличие системы
гарантированного
электропитания;

10) Наличие системы
заземления;

11) Соблюдение
требования по
проведению на
регулярной основе

инвентаризации серверного оборудования с проверкой его конфигурации; 12) Соблюдение требования по размещению серверного оборудования аппаратно-программного комплекса системы хранения данных в серверном помещении; 13) Соблюдение требования по расположению серверного помещения в отдельных, непроходных помещениях без оконных проемов. В случае наличия оконных проемов, они закрываются или заделываются негорючими материалами. Для поверхности стен, потолков и пола применяются материалы, не выделяющие и не накапливающие пыль; 14) Наличие фальшпола и (или) фальшпотолка для размещения кабельных систем и инженерных коммуникаций; 15) Соблюдение требования по исключению прохождение любых транзитных коммуникаций; 16) Соблюдение требования по расположению основных и резервных серверных помещений на безопасном расстоянии в удаленных друг от друга зданиях. Требования к резервным серверным помещениям идентичны требованиям к основным серверным помещениям.			
---	--	--	--

26	Соблюдение следующих требований по кроссовому помещению: 1) Отсутствие мощных источников электромагнитных помех; 2) Отсутствие труб и вентилей системы водоснабжения; 3) Наличие систем пожарной безопасности; 4) Отсутствие легко возгораемых материалов; 5) Наличие отдельной линии электропитания от отдельного автомата для подключения шкафа по проекту; 6) Наличие систем охранной сигнализации, контроля доступа; 7) Наличие системы кондиционирования.		
27	Соблюдение требования использования на этапе опытной и промышленной эксплуатации цифровых объектов средств и систем: мониторинга и управления инцидентами и событиями кибербезопасности; цифровой инфраструктурой; обнаружения и предотвращения вторжений.		
28	Соблюдение требования по созданию собственного центра обеспечения кибербезопасности и обеспечению его функционирования или приобретению услуг центра обеспечения кибербезопасности у третьих лиц, а также взаимодействие его с Национальным координационным		

	центром кибербезопасности.		
29	Соблюдение требований по размещению на Интернет-ресурсе с зарегистрированным доменным именем .KZ и (или) .ҚАЗ на аппаратно-программном комплексе, который расположен на территории Республики Казахстан. использованию доменных имен .KZ и (или) .ҚАЗ в пространстве казахстанского сегмента Интернета при передаче данных интернет-ресурсами с применением сертификатов безопасности.		
30	Соблюдение ГО, МИО и организацией требования по приобретению товаров в целях реализации требований обеспечения кибербезопасности для обороны страны и безопасности государства из реестра доверенного программного обеспечения и продукции электронной промышленности.		
	Соблюдение требований по контролю событий нарушений кибербезопасности в ГО, МИО или организации: 1) проведение мониторинга событий, связанных с нарушением кибербезопасности, и анализ результатов мониторинга; 2) регистрация события, связанные с состоянием кибербезопасности, и выявляются нарушения путем анализа журналов событий, в том числе:		

журналов событий
операционных систем;
журналов событий
систем управления
базами данных;
журналов событий
антивирусной защиты;
журналов событий
прикладного ПО;
журналов событий
телекоммуникационного
оборудования;
журналов событий
систем обнаружения и
предотвращения атак;
журналов событий
системы управления
контентом;
3) обеспечение
синхронизации времени
журналов регистрации
событий с
инфраструктурой
источника времени;
4) хранение журналов
регистрации событий в
течение срока,
указанного в ТД по
обеспечению
кибербезопасности, но не
менее трех лет и
нахождения в
оперативном доступе не
менее двух месяцев;
5) ведение журналов
регистрации событий;
6) обеспечение защиты
журналов регистрации
событий от
вмешательства и
неавторизованного
доступа. Не допущение
наличие у системных
администраторов
полномочий на
изменение, удаление и
отключение журналов.
Для конфиденциальных
ЦС требуются создание и
ведение резервного
хранилища журналов;
7) обеспечение внедрения
формализованной

	процедуры информирования об инцидентах кибербезопасности и реагирования на инциденты кибербезопасности.		
32	Соблюдение требования по наличию соглашения, в котором устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение при привлечении сторонних организаций к обеспечению кибербезопасности ЦР, ЦС, цифровой инфраструктуры.		
33	Соблюдение требований при внесении изменений в условия трудового договора работника организации, ротации или продвижении по государственной службе служащего ГО, МИО, их увольнении права доступа к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего служащего ГО, МИО или работника организации, аннулируются.		
34	Соблюдение требования организации и ведения учета прохождения служащими ГО, МИО или работниками организаций повышения обучения в сфере цифровизации и области обеспечения		

	кибербезопасности с выдачей электронного сертификата, обеспечением хранения в материалах личного дела кадровой службой.		
35	Соблюдение требований по регистрации в службе реагирования на компьютерные инциденты государственной технической службы, события кибербезопасности идентифицированных как критические для конфиденциальности, доступности и целостности по результатам анализа мониторинга событий кибербезопасности и анализа журнала событий .		
36	Соблюдение требования по проведению аудита кибербезопасности не реже одного раза в год, владельцам критически важных цифровых объектов, обрабатывающих данные , содержащие охраняемую законом тайну.		
37	Соблюдение требования по наличию протоколов с положительным результатом испытаний на соответствие требованиям кибербезопасности.		
38	Соблюдение требований по обеспечению разрабатываемого или приобретаемого готового прикладного ПО интерфейсом пользователя, ввод, обработку и вывод данных на казахском, русском и других языках,		

	по необходимости, с возможностью выбора пользователем языка интерфейса.		
39	Соблюдение требований по осуществлению мониторинга: действий пользователей и персонала; использования средств обработки информации.		
40	Соблюдение требования по обеспечению разрабатываемого или приобретаемого готового прикладного ПО технической документацией по эксплуатации на казахском и русском языках.		
41	Соблюдение требований по обеспечению высокой доступности сервера встроенных систем: 1) горячей замены резервных вентиляторов, блоков питания, дисков и адаптеров ввода-вывода; 2) оповещения о критических событиях; 3) поддержки непрерывного контроля состояния критичных компонентов и измерения контролируемых показателей.		
42	Соблюдение требований по наличию программного и аппаратного обеспечения гарантированного уничтожения информации при выводе из эксплуатации носителей информации, используемых в конфиденциальных ЦС, конфиденциальных ЦР и ЦР, содержащих персональные данные ограниченного доступа.		

43	Соблюдение требования по наличию документированной схемы локальной сети, которая поддерживается в актуальном состоянии при эксплуатации.		
44	Соблюдение требований по применению системы предотвращения утечки данных (DLP) для защиты цифровых объектов ГО, МИО и критически важных цифровых объектов При этом обеспечиваются: визуальное уведомление пользователя о проводимом контроле действий; размещение центра управления и серверов системы предотвращения утечки данных в пределах локальной сети.		
45	Соблюдение требований по интеграции ЦС ГО или МИО, в том числе с ЦС ГО и МИО, находящейся в опытной эксплуатации.		
46	Соблюдение требований по не допущению подключения к единой транспортной среде государственных органов (далее - ЕТС ГО), локальной сети цифровых субъектов, а также техническим средствам, входящим в состав ЕТС ГО, локальной сети цифровых субъектов, устройств для организации удаленного доступа посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи		

	, абонентских устройств сотовой связи и других беспроводных сетевых устройств, за исключением организованных оператором "цифрового правительства" беспроводных каналов связи ЕТС ГО, с использованием СКЗИ.		
47	Соблюдение требования по вводу в промышленную эксплуатацию цифрового объекта "цифрового правительства" осуществляется его собственником или владельцем только с использованием исполняемых кодов, скомпонованных из исходных кодов цифровых объектов "цифрового правительства", переданных ему государственной технической службой.		
48	Соблюдение требования по исключению подключения ЛС внутреннего контура цифровых субъектов к Интернету.		
49	Соблюдение требования по обеспечению собственником и (или) владельцем интернет-ресурса создания общедоступных интернет ресурсов на казахском, русском и, по необходимости, на других языках, с возможностью выбора пользователем языка интерфейса.		
	Соблюдение требований по вводу в промышленную эксплуатацию ЦС ГО, МИО и организаций в		

50	соответствии с требованиями технической документации при условии положительного завершения опытной эксплуатации, наличия протоколов испытаний с положительными результатами испытаний на соответствие требованиям кибербезопасности, подписания акта о вводе в промышленную эксплуатацию ЦС приемочной комиссией с участием представителей уполномоченных органов в сферах цифровизации и обеспечения кибербезопасности, заинтересованных ГО, МИО и организаций.		
----	--	--	--

Должностное (ые) лицо (а) _____

должность

подпись

фамилия, имя, отчество (при наличии)

Руководитель субъекта контроля _____

должность

подпись

фамилия, имя, отчество (при наличии)