



Правила формирования и утверждения системы управления рисками и внутреннего контроля, а также предоставления информации о системе управления рисками и внутреннего контроля операторами связи

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 31 июля 2026 года № 443/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 31 июля 2026 года № 39467

В соответствии со статьей 39-3 Закона Республики Казахстан "О связи"
ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила формирования и утверждения системы управления рисками и внутреннего контроля, а также предоставления информации о системе управления рисками и внутреннего контроля операторами связи.

2. Комитету телекоммуникаций Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) размещение настоящего 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 приказа представление в Юридический департамент Министерства искусственного интеллекта и цифрового развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

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

*Заместитель Премьер-Министра –
Министр искусственного интеллекта и
цифрового развития Республики Казахстан*

Ж. Мадиев

"СОГЛАСОВАН"

Комитет национальной безопасности
Республики Казахстан

"СОГЛАСОВАН"

Правила формирования и утверждения системы управления рисками и внутреннего контроля, а также предоставления информации о системе управления рисками и внутреннего контроля операторами связи

Глава 1. Общие положения

1. Настоящие Правила формирования и утверждения системы управления рисками и внутреннего контроля, а также предоставления информации о системе управления рисками и внутреннего контроля оператором связи (далее – Правила) разработаны в соответствии со статьей 39-3 Закона Республики Казахстан "О связи" и определяют порядок формирования и утверждения системы управления рисками и внутреннего контроля, а также предоставления информации о системе управления рисками и внутреннего контроля операторами связи (далее – СУРиВК).

2. Действие настоящих Правил распространяется на операторов связи, формирующих и утверждающих СУРиВК, а также предоставления информации о СУРиВК оператором связи уполномоченному органу в области связи, предусматривающие мероприятия направленные на обеспечение качества услуг связи и предотвращению мошенничества на сетях связи.

3. Основные понятия, используемые в настоящих Правилах:

1) оператор связи – физическое или юридическое лицо, зарегистрированное на территории Республики Казахстан, оказывающее услуги связи и (или) эксплуатирующее сети связи;

2) риск – вероятность возникновения событий, связанных с деятельностью оператора связи, способных оказать негативное влияние на соблюдение требований законодательства Республики Казахстан, качество услуг связи и предотвращение мошенничества на сетях связи;

3) услуги связи - деятельность по приему, обработке, хранению, передаче, перевозке, доставке почтовых и специальных отправок, почтовых переводов денег или сообщений телекоммуникаций;

4) несанкционированный трафик (фрод) - трафик, пропускаемый в нарушение установленных правил присоединения и взаимодействия сетей телекоммуникаций, включая пропуск трафика и порядок взаиморасчетов, в том числе трафик с подменой номера вызывающего абонента;

5) уполномоченный орган в области связи (далее – уполномоченный орган) - центральный исполнительный орган, определяемый Правительством Республики Казахстан, осуществляющий реализацию государственной политики в области связи, государственный контроль, координацию и регулирование деятельности лиц, предоставляющих услуги в области связи или пользующихся ими.

4. При формировании и функционировании СУРиВК оператор связи руководствуется международными и национальными стандартами Республики Казахстан в области менеджмента риска, в том числе:

- 1) СТ РК ISO 31000–2020 "Менеджмент риска. Руководящие указания";
- 2) СТ РК ИЕС 31010–2020 "Менеджмент риска. Методы оценки риска";
- 3) СТ РК ИСО Руководство 73–2010 "Менеджмент риска. Словарь".

Глава 2. Порядок формирования и утверждения системы управления рисками и внутреннего контроля

5. Оператор связи формируют СУРиВК с учетом характера, масштаба и сложности осуществляемой деятельности.

6. СУРиВК функционирует на постоянной основе и является неотъемлемой частью процессов управления и принятия решений оператором связи.

7. При формировании СУРиВК оператор связи обеспечивает:

1) определение полномочий, ответственности, порядка взаимодействия и координации структурных подразделений и (или) должностных лиц ответственных за управление рисками и внутреннего контроля;

2) документирование процессов СУРиВК, включая ведение реестра рисков в соответствии с внутренними документами;

3) проведение мониторинга эффективности СУРиВК и принятие мер по ее совершенствованию;

4) пересмотр и актуализацию СУРиВК не реже одного раза в год;

5) внеплановый пересмотр СУРиВК при изменении действующего законодательства Республики Казахстан, организационной структуры, внедрении новых технологий, а также при реализации существенных рисков.

8. Структурные подразделения и (или) должностные лица, ответственные за управление рисками и внутренний контроль, подотчетны руководителю оператора связи либо должностному лицу, определяемому внутренним документом оператора связи.

9. В целях эффективного и качественного формирования и управления СУРиВК оператор связи выстраивает "три линии защиты":

1) "первая линия защиты" осуществляется всеми структурными подразделениями оператора связи, ответственных за выявление, оценку, мониторинг и минимизацию рисков в рамках осуществляемой деятельности.

2) "вторая линия защиты" осуществляется структурными подразделениями оператора связи ответственных за управление рисками, внутренний контроль, кибербезопасность, комплаенс и иные контрольные функции.

Для структурных подразделений и (или) должностных лиц оператора связи, ответственных за управление рисками и внутренний контроль, предоставляется доступ к информации, необходимой для выполнения возложенных функций, включая сведения ограниченного доступа, в соответствии с действующим законодательством Республики Казахстан.

3) "третья линия защиты" осуществляется подразделением внутреннего аудита либо иными лицами, выполняющими функции независимой оценки эффективности СУРиВК в порядке, установленном внутренними документами оператора связи.

10. К основным категориям рисков в рамках настоящих Правил относятся:

1) риск нарушения непрерывности оказания услуг связи – риск возникновения чрезвычайных, аварийных, технологических и иных событий, способных привести к существенному нарушению либо прекращению оказания услуг связи и требующих применения мер по обеспечению непрерывности деятельности;

2) риск качества услуг связи – риск возникновения событий, способных оказать негативное влияние на достижение целевых параметров качества услуг связи, соблюдение требований законодательства Республики Казахстан и выполнение обязательств перед абонентами;

3) риск мошеннических действий на сетях связи – риск возникновения событий, связанных с совершением мошеннических действий на сетях связи, включая несанкционированный трафик (фрод), подмену абонентских номеров, несанкционированный доступ к услугам связи и иные противоправные действия, способные привести к финансовым потерям, нарушению качества услуг связи и причинению вреда абонентам;

4) правовой (комплаенс) риск – риск возникновения потерь вследствие несоблюдения или ненадлежащего применения требований законодательства Республики Казахстан, договорных обязательств и внутренних документов оператора связи, а также вследствие изменений законодательства, неоднозначного толкования норм и различной правоприменительной практики.

Операторы связи определяют иные категории рисков с учетом характера, масштаба и сложности осуществляемой деятельности.

11. Оператор связи обеспечивает идентификацию, оценку и мониторинг рисков, а также ведение реестра рисков.

12. Для каждого риска определяется ответственный сотрудник структурного подразделения, отвечающий за его мониторинг и реализацию мероприятий по минимизации риска (далее – владелец риска).

13. Реестр рисков содержит описание риска, факторы риска, возможные последствия, владельца риска, оценку риска и мероприятия по его минимизации.

14. Оператор связи использует ключевые индикаторы риска для мониторинга факторов риска и своевременного принятия мер реагирования.

15. Оператор связи определяет допустимый уровень риска (риск-аппетит) с учетом особенностей своей деятельности.

16. Реестр рисков подлежит пересмотру и актуализации не реже одного раза в год.

17. Риски подлежат рассмотрению руководством оператора связи в порядке, установленном внутренними документами оператора связи.

18. При реализации рисков либо превышения допустимого уровня риска обеспечивается эскалация информации уполномоченным должностным лицам оператора связи.

При реализации риска либо превышении допустимого уровня риска уполномоченное должностное лицо оператора связи принимает решение о необходимости информирования уполномоченного органа в порядке, установленном внутренними документами оператора связи.

Уполномоченный орган направляет оператору связи рекомендации (разъяснения) касательно реализации СУРиВК, в том числе выявления и минимизации рисков.

19. Оператор связи ведет учет и анализ реализованных рисков и инцидентов в целях предупреждения повторных событий и совершенствования СУРиВК.

20. СУРиВК утверждается руководителем оператора связи или иным должностным лицом, определяемым внутренним документом оператора связи.

Глава 3. Порядок предоставления информации о системе управления рисками и внутреннего контроля

21. Уполномоченный орган направляет оператору связи запрос о предоставлении документов, сведений и пояснений, относящихся к СУРиВК (далее – запрос), посредством цифровых систем, интернет-ресурсов государственного органа, а также иными доступными способами.

22. В запросе указываются:

- 1) цель запроса;
- 2) перечень необходимых документов, сведений и (или) пояснений;
- 3) срок предоставления ответа.

23. Оператор связи предоставляет сведения и (или) пояснения по запросу уполномоченного органа в срок, не превышающий 30 календарных дней со дня получения запроса.

