

Об утверждении Правил порядка приостановления оказания услуг связи при выявлении инцидентов кибербезопасности

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 24 сентября 2026 года № 569/НК.
Зарегистрирован в Министерстве юстиции Республики Казахстан 29 сентября 2026 года № 39991

В соответствии с подпунктом 3) статьи 8-1 Закона Республики Казахстан "О связи" **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемые Правила порядка приостановления оказания услуг связи при выявлении инцидентов кибербезопасности.

2. Комитету по информационной безопасности 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 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.

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 Ж. Мадиев
Республики Казахстан*

"СОГЛАСОВАНО"

Комитет национальной безопасности
Республики Казахстан

Утверждены приказом
Заместитель Премьер-Министра –
Министр искусственного

Правила порядка приостановления оказания услуг связи при выявлении инцидентов кибербезопасности

Глава 1. Общие положения

1. Настоящие Правила порядка приостановления оказания услуг связи при выявлении инцидентов кибербезопасности (далее – Правила) разработаны в соответствии с подпунктом 3) статьи 8-1 Закона Республики Казахстан "О связи" и определяют порядок приостановления оказания услуг связи при выявлении инцидентов кибербезопасности.

2. В настоящих Правилах используются следующие основные понятия:

1) угроза кибербезопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности;

2) событие кибербезопасности – идентифицированное возникновение состояния цифрового объекта, указывающее на возможное нарушение кибербезопасности или ранее неизвестную ситуацию, которая может иметь отношение к обеспечению кибербезопасности;

3) приостановление оказания услуг связи при выявлении инцидентов кибербезопасности (далее – приостановление оказания услуг связи) – ограничение доступа к Интернету абонентского устройства связи.

4) инцидент кибербезопасности – событие или совокупность событий, негативно влияющих на кибербезопасность цифрового объекта;

5) Национальный координационный центр кибербезопасности (далее - НКЦКБ) – субъект, осуществляющий координацию деятельности по реагированию на инциденты кибербезопасности в соответствии с законодательством Республики Казахстан;

6) платформа информационного взаимодействия НКЦКБ (далее – платформа) – программное обеспечение, предназначенное для обмена данными и информацией об угрозах и инцидентах кибербезопасности с НКЦКБ;

7) центр обеспечения кибербезопасности – юридическое лицо или структурное подразделение юридического лица, являющееся резидентом Республики Казахстан без участия иностранных юридических и физических лиц, осуществляющее деятельность по защите цифровых объектов;

8) реагирование на инцидент кибербезопасности – действия, предпринятые для минимизации или устранения инцидента кибербезопасности, включая действия, предпринятые для защиты и восстановления штатного функционирования цифровых

объектов и цифровых данных, находящихся в них, процесс, включающий в себя выявление, анализ и принятие мер для противодействия событиям или нарушениям, которые могут представлять угрозу кибербезопасности цифровых объектов;

9) индикатор компрометации – технический признак, позволяющий выявить возможное наличие или последствия инцидента кибербезопасности.

3. Действие настоящих Правил распространяется на операторов связи, осуществляющих деятельность на территории Республики Казахстан.

4. Основанием для рассмотрения вопроса о приостановлении оказания услуг связи является информация об инциденте кибербезопасности, который приводит к нарушению функционирования сетей связи либо угрозе кибербезопасности, поступившая от центра обеспечения кибербезопасности либо от НКЦКБ.

Глава 2. Порядок приостановления оказания услуг связи при выявлении инцидентов кибербезопасности

5. Операторы связи в соответствии с пунктом 7 Национального антикризисного плана реагирования на инциденты кибербезопасности, утвержденного постановлением Правительства Республики Казахстан от 9 августа 2018 года № 488, разрабатывают и утверждают планы реагирования.

6. В целях эффективного взаимодействия операторы связи определяют ответственных должностных лиц за обеспечение кибербезопасности. Контактные данные должностных лиц направляются в НКЦКБ. Обо всех случаях замены ответственного должностного лица оператора связи либо его контактных данных НКЦКБ информируется в течение 48 (сорок восемь) часов.

7. Центр обеспечения кибербезопасности осуществляет круглосуточный мониторинг обеспечения кибербезопасности сетей связи.

8. При обнаружении инцидента кибербезопасности НКЦКБ направляет информацию в центр обеспечения кибербезопасности и оператору связи в соответствии с Правилами обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности, утвержденными приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НК (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 16886).

9. Информация об инциденте кибербезопасности направляется в электронной форме посредством платформы в течение 24 (двадцать четыре) часов с момента получения информации об инциденте кибербезопасности и содержит:

- 1) описание инцидента;
- 2) предполагаемое время начала;
- 3) затронутые сегменты сети;

4) предполагаемые последствия;

5) принятые меры реагирования.

10. Оператор связи обязан ограничить доступ к Интернету абонентскому устройству связи:

при неустранении абонентом выявленных оператором связи инцидентов кибербезопасности, которые могут привести к приостановлению услуг связи;

при поступлении информации об инциденте кибербезопасности от НКЦКБ, службы реагирования на инциденты кибербезопасности, оперативного центра кибербезопасности об инцидентах кибербезопасности, которые могут привести к приостановлению функционирования критически важных цифровых объектов.

11. Оператор связи уведомляет абонента в виде короткого текстового сообщения (далее – сообщение) о необходимости устранения выявленного инцидента кибербезопасности.

12. В случае неустранения абонентом инцидента кибербезопасности в течение 48 (сорок восемь) часов со дня направления оператором связи сообщения, оператор связи ограничивает доступ к Интернету абонентскому устройству связи. Сообщение оператора связи содержит информацию о факте выявления инцидента кибербезопасности и срок для устранения инцидентов кибербезопасности.

В случае неустранения абонентом инцидента кибербезопасности в течение 48 (сорок восемь) часов оказание услуг связи приостанавливается с момента получения сообщения от оператора связи.

13. К обстоятельствам, зависящим от оператора связи, относятся обстоятельства, возникшие вследствие его действий (бездействия), в том числе технические сбои или неисправности сети связи, оборудования либо программного обеспечения, используемых для направления и доставки сообщения.

К обстоятельствам, не зависящим от оператора связи, относятся обстоятельства, возникшие по вине абонента либо вследствие непреодолимой силы, препятствующие получению сообщения, в том числе отключение абонентского устройства связи, отсутствие в зоне действия сети связи, неисправность абонентского устройства связи либо иные обстоятельства, препятствующие получению сообщения.

Факт направления сообщения, дата и время его направления, а также результат его доставки подлежат фиксации оператором связи с использованием технических средств оператора связи.

14. Абонент принимает меры по устранению выявленного инцидента кибербезопасности на используемом им абонентском устройстве в срок, указанный в сообщении оператора связи.

15. По истечении срока, предоставленного абоненту для устранения инцидента, оператор связи проводит анализ наличия индикатора компрометации выявленного инцидента кибербезопасности.

16. В случае неустранения инцидента кибербезопасности абонентом, оператор связи приостанавливает оказание услуг связи и уведомляет НКЦКБ посредством платформы.

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