О внесении изменений в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ "Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности"

Приказ и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 25 июня 2026 года № 354/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 26 июня 2026 года № 39105

Примечание ИЗПИ!

Вводится в действие с 12.07.2026 г.

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ "Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 16886) следующие изменения:

заголовок изложить в следующей редакции:

"Об утверждении Правил обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности";

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 21) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" и подпунктом 292) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846 **ПРИКАЗЫВАЮ:**";

пункт 1 изложить в следующей редакции:

"1. Утвердить прилагаемые Правила обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности.";

Правила обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности, утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством 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 с 12 июля 2026 года и подлежит официальному опубликованию.

Исполняющий обязанности министра искусственного интеллекта и цифрового развития Республики Казахстан *Д. Мусалиев*

"СОГЛАСОВАНО"
Комитет национальной безопасности
Республики Казахстан

Приложение к приказу
Исполняющий обязанности
министра искусственного
интеллекта и цифрового развития
Республики Казахстан
от 25 июня 2026 года
№ 354/НҚ
Утверждены
приказом Министра
оборонной и аэрокосмической
промышленности
Республики Казахстан
от 19 марта 2018 года № 48/НҚ

Правила обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности

Глава 1. Общие положение

1. Настоящие Правила обмена информацией, необходимой для обеспечения кибербезопасности между, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности (далее – Правила) разработаны в соответствии с подпунктом 21) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" (далее – Закон) и подпунктом 292) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846 и определяют порядок взаимодействия Национального координационного центра кибербезопасности с центрами обеспечения кибербезопасности и отраслевыми центрами кибербезопасности при обмене информацией, необходимой для обеспечения кибербезопасности и реагирования на инциденты кибербезопасности.

2. В настоящих Правилах используются следующие основные понятия:

1) критически важные цифровые объекты (далее – КВЦО) – цифровые объекты, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, возникновению чрезвычайных ситуаций социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения , связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, "цифрового правительства";

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

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

4) уполномоченный орган в сфере обеспечения кибербезопасности (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения кибербезопасности;

5) Национальный координационный центр кибербезопасности (далее – НКЦКБ) – структурное подразделение акционерного общества "Государственная техническая служба";

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

7) центр обеспечения кибербезопасности (далее – ЦОК) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите цифровых ресурсов, цифровых систем, сетей телекоммуникаций и других цифровых объектов;

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

9) органы национальной безопасности Республики Казахстан (далее – органы национальной безопасности) – непосредственно подчиненные и подотчетные Президенту Республики Казахстан специальные государственные органы, являющиеся составной частью системы обеспечения безопасности Республики Казахстан и предназначенные в пределах предоставленных им полномочий, обеспечивать безопасность личности и общества, защиту конституционного строя, государственного суверенитета, территориальной целостности, экономического, научно-технического и оборонного потенциала страны;

10) уязвимость цифровых объектов – недостаток в программном или аппаратном обеспечении, обуславливающий возможность нарушения его работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном или аппаратном обеспечении;

11) кибербезопасность в сфере цифровизации (далее – кибербезопасность) – состояние защищенности цифровых ресурсов, цифровых систем и цифровой инфраструктуры от внешних и внутренних угроз;

12) цифровые объекты "цифрового правительства" (далее ЦО ЦП) – государственные электронные информационные ресурсы, программное обеспечение государственных органов, интернет-ресурс государственного органа, объекты цифровой инфраструктуры цифрового правительства", в том числе цифровые объекты иных лиц, предназначенные для формирования государственных цифровых ресурсов, осуществления государственных функций и оказания государственных услуг.

Главы 2. Порядок обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности

3. Участниками информационного обмена, необходимого для обеспечения кибербезопасности являются:

1) органы национальной безопасности;

2) уполномоченный орган;

3) НКЦКБ;

4) ЦОК.

4. ЦОК и НКЦКБ осуществляют обмен информацией, для выполнения возложенных на них задач и функций в сфере кибербезопасности.

5. ЦОК обеспечивают доведение полученной от НКЦКБ информации до обслуживаемых ими организаций и в свои структурные подразделения, обеспечивающие сопровождение инфраструктуры, в части их касающейся информации .

6. ЦОК и НКЦКБ необходимо осуществлять взаимодействие в интересах решения задач, направленных на:

1) совершенствование механизмов предотвращения нарушений кибербезопасности;

2) улучшение деятельности ЦОК;

3) повышение оперативности и согласованности действий между ЦОК и НКЦКБ;

4) выработку совместных решений по повышению уровня кибербезопасности цифровых объектов;

7. Информация, необходимая для обеспечения кибербезопасности, относится к категории конфиденциальных цифровых данных, получение, обработка и использование которых ограничивается целями, для которых она собирается. Представление сведений от НКЦКБ в ЦОКБ и от ЦОК в НКЦКБ осуществляется в рамках настоящих Правил.

8. При обнаружении инцидента кибербезопасности ЦОК:

уведомляет НКЦКБ и собственника или владельца ЦО ЦП или КВЦО в течение 15 (пятнадцати) минут с момента подтверждения инцидента кибербезопасности;

направляет в НКЦКБ карточку инцидента кибербезопасности по форме, согласно приложению к настоящим Правилам в течение 72 (семидесяти двух) часов с момента подтверждения инцидента кибербезопасности.

При поступлении уведомления от НКЦКБ об угрозе кибербезопасности, событии кибербезопасности или инциденте кибербезопасности, ЦОК в течение 72 (семидесяти двух) часов с момента уведомления направляет в НКЦКБ:

результаты анализа угрозы кибербезопасности;

результаты анализа события кибербезопасности при подтверждении события кибербезопасности;

карточку инцидента кибербезопасности по форме, согласно приложению к настоящим Правилам при подтверждении инцидента кибербезопасности.

9. Сбор данных осуществляется:

1) при проведении анализа сведений по возникшим угрозам, уязвимостям и инцидентам кибербезопасности;

2) при наличии оснований полагать, что инцидент кибербезопасности способен повлиять на работоспособность цифровых ресурсов, цифровых систем, сетей телекоммуникаций и других цифровых объектов;

3) при распространении угрозы, уязвимости и инцидента кибербезопасности;

4) по запросу органа национальной безопасности, уполномоченного органа и НКЦКБ об угрозах, уязвимостях, событиях и инцидентах кибербезопасности;

5) при оказании помощи при устранении последствий инцидентов кибербезопасности.

10. ЦОК по запросу НКЦКБ обеспечивает доступ НКЦКБ к имеющимся системам мониторинга обеспечения кибербезопасности.

11. НКЦКБ оповещает заинтересованные стороны:

1) ЦОК в случае выявления угроз кибербезопасности, событий кибербезопасности или инцидентов кибербезопасности, которые способны повлиять на целостность, доступность, конфиденциальность цифровых ресурсов, цифровых систем, сетей телекоммуникаций и других цифровых объектов, в части касающейся их информации;

2) органы национальной безопасности в случае инцидентов кибербезопасности, связанных с цирфровыми ресурсами, цифровыми системами, сетями телекоммуникаций и другими цифровых объектами;

3) уполномоченный орган в случае нарушения законодательства в сфере кибербезопасности;

4) уполномоченный орган в сфере кибербезопасности Республики Казахстан в случае нарушения законодательства в сфере кибербезопасности;

5) органы прокуратуры Республики Казахстан в пределах их компетенции в случае нарушения соответствующего законодательства;

6) органы внутренних дел Республики Казахстан в пределах их компетенции в случае нарушения соответствующего законодательства.

12. Информационный обмен осуществляется следующими способами:

1) отправка данных в форматах расширенного языка разметки (eXtensible Markup Language – XML) или текстового формата обмена данными (JavaScript Object Notation – JSON) с помощью электронного сообщения с использованием шифрования;

2) отправка данных в форматах XML или JSON с использованием программного обеспечения для обмена информацией;

3) отправка зашифрованных данных с использованием протокола HTTPS (HyperText Transfer Protocol Secure);

4) отправка данных с использованием протоколов, согласованных к использованию уполномоченным органом.

13. Полученная в процессе информационного обмена информация используется исключительно в целях координации реагирования на инциденты кибербезопасности.

14. Обмен сообщениями осуществляется между НКЦКБ и ЦОК с использованием платформы НКЦКБ и отечественного сертификата шифрования.

15. ЦОК предоставляет контактные данные (адрес электронной почты, телефон доступный в режиме 24/7/365), а также ежеквартально, не позднее 10 числа первого месяца квартала, подтверждает, обновляет и направляет контактные данные в НКЦКБ. В случае изменения контактных данных, оперативно информирует НКЦКБ.

16. ЦОК ежеквартально, в срок до 10 числа месяца, следующего за отчетным кварталом, предоставляет в НКЦКБ информацию об инцидентах кибербезопасности, зарегистрированных за отчетный квартал, и о мерах, принятых для устранения причин их возникновения.

Приложение
к Правилам обмена
информацией, необходимой для
обеспечения кибербезопасности,
между центрами обеспечения
кибербезопасности и
Национальным
координационным центром
кибербезопасности
Форма

Карточка инцидента кибербезопасности

Дата регистрации инцидента кибербезопасности	
Уровень критичности инцидента кибербезопасности	Высокий (4); Средний (3); Низкий (2); Не определено (1).
Тип инцидента кибербезопасности	Отказ в облуживании (DoS, DDoS); Несанкционированный доступ и модификация содержания; Ботнет; Вирусная атака; Шифровальщик; Эксплуатация уязвимости; Компрометация средств аутентификации/ авторизации; Фишинг; Спам; Иные инциденты информационной безопасности.
Масштабность	Единичный; Массовый.
Детали	Дата и время возникновения; Дата и время подтверждения;

	Повторный/новый; Индикатор компрометации (IOC).
Признак	Действительный; Попытка; Подозрение;
Контур	Локальная сеть внутреннего контура; Локальная сеть внешнего контура.
Описание инцидента кибербезопасности	
Последствие	Без последствий; Нарушение работоспособности; Нарушение целостности; Нарушение режима конфиденциальности информации.
Объект, которому нанесен ущерб	
Действия, предпринятые для устранения инцидента кибер безопасности	
Примечание	

Уровни критичности инцидента информационной безопасности

Уровень критичности	Признаки	Примеры инцидентов информационной безопасности
Высокий (4)	инциденты кибербезопасности, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных данных, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего критичные данные.	-Несанкционированный доступ -Эксплуатация уязвимости -Шифровальщик -Вредоносное программное обеспечение -Отказ в обслуживании (DoS/ DDoS-атака) -Иные инциденты кибербезопасности
Средний (3)	инциденты кибербезопасности, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/ модификации данных, не являющихся критичными, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего данные, не являющихся критичными.	-Несанкционированный доступ -Шифровальщик -Вредоносное программное обеспечение -Отказ в обслуживании (DoS/ DDoS-атака) -Эксплуатация уязвимости -Иные инциденты информационной безопасности
Низкий (2)	инциденты кибербезопасности, не влияющие на предоставление услуг/выполнение работ.	-Вредоносное программное обеспечение -Отказ в обслуживании (DoS/ DdoS-атака) -Эксплуатация уязвимости -Спам -Фишинговая атака

		-Иные инциденты информационной безопасности
Не определено (1) *	Влияние инцидента кибербезопасности на предоставление услуг не определено	Нехарактерная/подозрительная активность

Примечание:

* Уровень необходимо пересмотреть в течение 48 (сорока восьми) часов с момента подтверждения инцидента кибербезопасности.