О внесении изменений и дополнений 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 Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 14 января 2026 года № 17/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 19 января 2026 года № 37856

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 за № 16886), следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 19) статьи 7-1 Закона Республики Казахстан "Об информатизации" 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:**";

в Правилах обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности, утвержденных указанным приказом:

пункт 1 изложить в следующей редакции:

"1. Настоящие Правила обмена информацией, необходимой для обеспечения информационной безопасности между, оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности (далее – Правила) разработаны в соответствии с подпунктом 19) статьи 7-1 Закона Республики Казахстан "Об информатизации" (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 информационной безопасности с оперативными центрами обеспечения информационной безопасности при обмене информацией, необходимой для обеспечения информационной безопасности и реагирования на инциденты информационной безопасности.";

в пункте 2:

дополнить подпунктом 2-1) следующего содержания:

"2-1) критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ) – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации 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, "электронного правительства";";

дополнить подпунктом 11) следующего содержания:

"11) объекты информатизации "электронного правительства" (далее ОИ ЭП) – государственные электронные информационные ресурсы, программное обеспечение государственных органов, интернет-ресурс государственного органа, объекты информационно-коммуникационной инфраструктуры "электронного правительства", в том числе объекты информатизации иных лиц, предназначенные для формирования государственных электронных информационных ресурсов, осуществления государственных функций и оказания государственных услуг.";

пункт 9 изложить в следующей редакции:

"9. При обнаружении инцидента информационной безопасности ОЦИБ:

уведомляет НКЦИБ и собственника или владельца ОИ ЭП или КВОИКИ в течение 15 (пятнадцати) минут с момента подтверждения инцидента информационной безопасности;

направляет в НКЦИБ карточку инцидента информационной безопасности по форме, согласно Приложению 3 к настоящим Правилам в течение 72 (семидесяти двух) часов с момента подтверждения инцидента информационной безопасности.

При поступлении уведомления от НКЦИБ об угрозе информационной безопасности , событии информационной безопасности или инциденте информационной

безопасности, ОЦИБ в течение 72 (семидесяти двух) часов с момента уведомления направляет в НКЦИБ:

результаты анализа угрозы информационной безопасности;

результаты анализа события информационной безопасности при подтверждении события информационной безопасности;

карточку инцидента информационной безопасности по форме, согласно приложению 3 к настоящим Правилам при подтверждении инцидента информационной безопасности.";

подпункт 1) пункта 12 изложить в следующей редакции:

"1) ОЦИБ в случае выявления угроз информационной безопасности, событий информационной безопасности или инцидентов информационной безопасности, которые способны повлиять на целостность, доступность, конфиденциальность электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и объектов информатизации, в части касающейся их информации;";

подпункт 2) пункта 13 изложить в следующей редакции:

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

дополнить приложением 3 согласно приложению, 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 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

Приложение к приказу
Заместитель Премьер-Министра
– Министр искусственного интеллекта
и цифрового развития
Республики Казахстан
от 14 января 2026 года № 17/НҚ

Приложение 3
к Правилам обмена информацией,
необходимой для обеспечения
информационной безопасности,
между оперативными центрами
обеспечения информационной
безопасности и Национальным
координационным центром
информационной безопасности

Форма

Карточка инцидента информационной безопасности

Дата регистрации инцидента информационной безопасности	
Уровень критичности инцидента информационной безопасности	Высокий (4); Средний (3); Низкий (2); Не определено (1).
Тип инцидента информационной безопасности	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).
	Действительный;

Признак	Попытка; Подозрение;
Контур	Локальная сеть внутреннего контура; Локальная сеть внешнего контура.
Описание инцидента информационной безопасности	
Последствие	Без последствий; Нарушение работоспособности; Нарушение целостности; Нарушение режима конфиденциальности информации.
Объект, которому нанесен ущерб	
Действия, предпринятые для устранения инцидента информационной безопасности	
Примечание	

Уровни критичности инцидента информационной безопасности

Уровень критичности	Признаки	Примеры инцидентов информационной безопасности
Высокий (4)	инциденты информационной безопасности, 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 информационной безопасности
Средний (3)	инциденты информационной безопасности, 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 информационной безопасности, 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
	Влияние инцидента информационной безопасности на	

Не определено (1) *	предоставление услуг не определено	Нехарактерная/подозрительная активность

Примечание:

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