

Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 11 мая 2018 года № 16886.

В соответствии с подпунктом 19) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности.

2. Комитету по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) в течение десяти календарных дней со дня государственной регистрации в Министерстве юстиции Республики Казахстан настоящего приказа направление его копии в бумажном и электронном виде на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) в течение десяти календарных дней после государственной регистрации настоящего приказа направление его копии на официальное опубликование в периодические печатные издания;

4) размещение настоящего приказа на интернет-ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

5) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в

Юридический департамент Министерства оборонной и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2), 3) и 4) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра оборонной и аэрокосмической промышленности Республики Казахстан.

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

*Министр оборонной и
аэрокосмической промышленности
Республики Казахстан*

Б. Атамкулов

Утверждены
приказом Министра оборонной и
аэрокосмической промышленности
Республики Казахстан
от 19 марта 2018 года № 48/НК

Правила обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности

Глава 1. Общие положения

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 от 24 ноября 2015 года "Об информатизации" (далее – Закон) 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.

2. В настоящих Правилах используются следующие основные понятия:

1) уязвимость объекта информатизации – 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;

2) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

3) событие информационной безопасности – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;

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

5) Национальный координационный центр информационной безопасности (далее – НКЦИБ) – структурное подразделение акционерного общества "Государственная техническая служба";

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

7) оперативный центр информационной безопасности (далее – ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации ;

8) угроза информационной безопасности – действия способные оказать негативное воздействие на конфиденциальность, целостность и доступность объекта информатизации;

9) инцидент информационной безопасности – отдельно или серийно возникающий сбой в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

10) 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.

Сноска. Пункт 2 - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по

истечении десяти календарных дней после дня его первого официального опубликования).

Глава 2. Порядок обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности

Сноска. В заголовок главы 2 внесено изменение на казахском языке, текст на русском языке не изменяется приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

3. Участниками информационного обмена, необходимого для обеспечения информационной безопасности являются:

- 1) органы национальной безопасности;
- 2) уполномоченный орган;
- 3) НКЦИБ;
- 4) ОЦИБ.

4. ОЦИБ и НКЦИБ осуществляют обмен информацией, необходимой для выполнения возложенных на них задач и функций в сфере информационной безопасности.

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

6. Исключен приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 31.03.2023 № 120/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

7. ОЦИБ и НКЦИБ необходимо осуществлять взаимодействие в интересах решения задач, направленных на:

- 1) совершенствование механизмов предотвращения нарушений информационной безопасности;
- 2) улучшение деятельности ОЦИБ;
- 3) повышение оперативности и согласованности действий между ОЦИБ и НКЦИБ;
- 4) выработку совместных решений по повышению уровня информационной безопасности объектов информатизации.

8. Информация, необходимая для обеспечения информационной безопасности, относится к категории конфиденциальных электронных информационных данных, получение, обработка и использование которых ограничивается целями, для которых

она собирается. Представление сведений от НКЦИБ в ОЦИБ и от ОЦИБ в НКЦИБ осуществляется в рамках настоящих Правил.

Сноска. В пункт 8 внесено изменение на казахском языке, текст на русском языке не изменяется приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

9. ОЦИБ предоставляет информацию об инцидентах информационной безопасности в НКЦИБ в течение 15 минут с момента его подтверждения.

Сноска. Пункт 9 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 31.03.2023 № 120/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

10. Сбор данных осуществляется:

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

2) при наличии оснований полагать, что инцидент информационной безопасности способен повлиять на работоспособность электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации ;

3) при распространении угрозы, уязвимости и инцидента информационной безопасности;

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

5) при оказании помощи при устранении последствий инцидентов информационной безопасности.

11. ОЦИБ по запросу НКЦИБ обеспечивает доступ НКЦИБ к имеющимся системам мониторинга обеспечения информационной безопасности.

12. НКЦИБ оповещает заинтересованные стороны:

1) ОЦИБ в случае инцидентов информационной безопасности, которые способны повлиять на работоспособность электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации , в части их касающейся информации;

2) органы национальной безопасности в случае инцидентов информационной безопасности, связанных с электронными информационными ресурсами, информационными системами, сетями телекоммуникаций и другими объектами информатизации;

3) уполномоченный орган в случае нарушения законодательства в сфере информационной безопасности;

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

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.

13. Информационный обмен осуществляется следующими способами:

1) отправка данных в форматах XML (eXtensible Markup Language – расширенный язык разметки) или JSON (JavaScript Object Notation – текстовый формат обмена данными) с помощью электронного сообщения с использованием шифрования;

2) вносится изменение на государственном языке, текст на русском языке не меняется;

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

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

Сноска. Пункт 13 - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

14. Исключен приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 31.03.2023 № 120/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

15. Полученная в процессе информационного обмена информация используется исключительно в целях координации реагирования на инциденты информационной безопасности.

16. Обмен сообщениями осуществляется между НКЦИБ и ОЦИБ с использованием платформы НКЦИБ и отечественного сертификата шифрования.

Сноска. Пункт 16 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 31.03.2023 № 120/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

17. ОЦИБ 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 НКЦИБ. В случае изменения контактных данных, незамедлительно информирует НКЦИБ.

18. ОЦИБ ежеквартально, в срок до 10 числа месяца, следующего за отчетным кварталом, предоставляет в НКЦИБ информацию об инцидентах информационной

безопасности, зарегистрированных за отчетный квартал, и о мерах, принятых для устранения причин их возникновения.

Сноска. Правила дополнены пунктом 18 в соответствии с приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Приложение 1
к Правилам обмена
информацией, необходимой для
обеспечения информационной
безопасности, между
оперативными центрами
обеспечения информационной
безопасности и Национальным
координационным центром
информационной безопасности

Сноска. Приложение 1 исключено приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Приложение 2
к Правилам обмена
информацией, необходимой для
обеспечения информационной
безопасности, между
оперативными центрами
обеспечения информационной
безопасности и Национальным
координационным центром
информационной безопасности

Сноска. Приложение 2 исключено приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 12.05.2021 № 164/НК (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).