

Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности

Постановление Правительства Республики Казахстан от 9 августа 2018 года № 488.

В соответствии с подпунктом 6-1) статьи 6 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемый Национальный антикризисный план реагирования на инциденты информационной безопасности.
2. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

*Премьер-Министр
Республики Казахстан*

Б. Сагинтаев

Утвержден
постановлением
Правительства
Республики Казахстан
от 9 августа 2018 года № 488

Национальный антикризисный план реагирования на инциденты информационной безопасности

Глава 1. Общие положения

1. Национальный антикризисный план реагирования на инциденты информационной безопасности (далее – план) определяет порядок действий субъектов системы по снижению влияния инцидентов информационной безопасности на состояние информационной безопасности с одновременным сведением к минимуму нарушений их работы.

2. Настоящий план не распространяется на информационные системы в защищенном исполнении, отнесенные к государственным секретам в соответствии с законодательством Республики Казахстан о государственных секретах, а также сети телекоммуникаций специального назначения и/или правительственный, президентской, засекреченной, шифрованной и кодированной связи.

3. В настоящем плане используются следующие понятия:

1) объекты информационно-коммуникационной инфраструктуры (далее – объекты ИКИ) – информационные системы, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

2) критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ) – объекты ИКИ, в том числе информационно-коммуникационной инфраструктуры "электронного правительства", нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории;

3) система реагирования на инциденты информационной безопасности (далее – система) – совокупность сил и средств обеспечения информационной безопасности, предназначенных для реализации общегосударственного комплекса мероприятий по защите электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от технологических сбоев или несанкционированного воздействия в результате компьютерных атак и ликвидации их последствий;

4) инцидент информационной безопасности (далее – инцидент ИБ) – отдельно или серийно возникающие сбои 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;

5) кризисная ситуация в сфере информационной безопасности – инцидент ИБ или реальные предпосылки к его возникновению на объектах ИКИ, которые могут привести к невозможности или ограничению предоставления государственных услуг, чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории;

6) национальный координационный центр информационной безопасности (далее – НКЦИБ) – структурное подразделение республиканского государственного предприятия на праве хозяйственного ведения "Государственная техническая служба" Комитета национальной безопасности Республики Казахстан;

7) субъекты системы – государственные органы, уполномоченные на решение вопросов информационной безопасности или реагирования на инциденты ИБ, НКЦИБ, Оперативный штаб, владельцы объектов информатизации "электронного правительства", владельцы КВОИКИ, оперативные центры информационной безопасности (далее – ОЦИБ), службы реагирования на инциденты информационной безопасности;

8) компьютерная атака – целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно-аппаратных средств (или протоколов межсетевого взаимодействия).

Иные понятия, применяемые в плане, соответствуют понятиям, используемым в законодательстве Республики Казахстан в области информатизации и связи.

Глава 2. Профилактические мероприятия

4. В целях профилактики и недопущения инцидентов в сфере информатизации и связи НКЦИБ на плановой основе проводит разъяснительные работы по инцидентам ИБ, для этого на постоянной основе осуществляет сбор, анализ и обобщение информации от субъектов системы и иных источников, включая иностранные и международные организации в сфере информационной безопасности.

5. ОЦИБ в целях выявления и пресечения угроз ИБ осуществляет мониторинг подключенной к нему информационно-коммуникационной инфраструктуры и объектов информатизации.

6. Взаимодействие ОЦИБ по вопросам мониторинга обеспечения информационной безопасности объектов информатизации обеспечивает НКЦИБ.

7. Субъекты системы для повышения уровня защищенности электронных информационных ресурсов, программного обеспечения, информационных систем и поддерживающей их информационно-коммуникационной инфраструктуры руководствуются Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, а также иными нормативными правовыми актами, регламентирующими сферу информационной безопасности.

Глава 3. Действия собственников и владельцев критически важных объектов информационно-коммуникационной инфраструктуры и объектов информатизации "электронного правительства"

8. В целях обеспечения реагирования на инциденты ИБ с уровнями критичности от 0 до 5 владельцы объектов информатизации "электронного правительства", владельцы КВОИКИ, ОЦИБ разрабатывают и утверждают планы реагирования, в которых предусматриваются меры по обработке угроз (рисков) информационной безопасности, обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации, и следующие обязательные мероприятия по:

- 1) организации и проведению мероприятий по недопущению возникновения кризисной ситуации информационной безопасности;
- 2) сбору и анализу данных о состоянии информационной безопасности в информационно-коммуникационной инфраструктуре;
- 3) осуществлению взаимодействия с ОЦИБ и НКЦИБ;
- 4) поддерживающим мерам обеспечения непрерывности работы и устойчивости к внешним изменениям;
- 5) информированию заинтересованных субъектов системы по вопросам обнаруженных инцидентов информационной безопасности и их устранению;
- 6) порядку действий при ликвидации инцидентов информационной безопасности и их последствий, минимизации воздействия на информационно-коммуникационную инфраструктуру субъекта системы;
- 7) мерам сохранения цифровых следов инцидентов информационной безопасности (журналов, отчетов и форм);
- 8) установлению причин инцидентов информационной безопасности;
- 9) действиям, которые должны быть предприняты после инцидента информационной безопасности;
- 10) устраниению причины инцидента ИБ;
- 11) процедурам восстановления.

Иные мероприятия могут быть включены, исходя из особенностей функционирования информационно-коммуникационной инфраструктуры и (или) технологических процессов субъектов системы.

9. Владельцы объектов информатизации "электронного правительства" и КВОИКИ направляют копию утвержденных планов реагирования на инциденты информационной безопасности в уполномоченный орган по обеспечению информационной безопасности.

10. По вопросам инцидентов ИБ собственники и владельцы КВОИКИ и объектов информатизации "электронного правительства" взаимодействуют с НКЦИБ посредством круглосуточного call-центра 1400 или официального сайта www.kz-cert.kz.

11. По решению владельцев объектов информатизации "электронного правительства", КВОИКИ к реагированию на инциденты информационной безопасности могут быть привлечены службы реагирования на инциденты информационной безопасности и (или) ОЦИБ.

12. Владельцы объектов информатизации "электронного правительства", КВОИКИ после завершения реагирования приступают к реализации предусмотренных планом мер по восстановлению системы, в том числе используя рекомендации уполномоченного органа по информационной безопасности и НКЦИБ.

13. В целях эффективного взаимодействия владельцы объектов информатизации "электронного правительства", КВОИКИ определяют ответственных должностных лиц за обеспечение информационной безопасности.

Контактные данные лиц направляются в НКЦИБ. Обо всех случаях замены ответственного должностного лица, либо его контактов НКЦИБ информируется в течение 48-и часов.

Глава 4. Реагирование на инциденты информационной безопасности

Параграф 4.1. Действия уполномоченных органов по реагированию на инциденты информационной безопасности

14. НКЦИБ в случаях получения информации об инцидентах информационной безопасности на объектах информатизации в соответствии с 3, 4 и 5 уровнями критичности инцидентов информационной безопасности, установленными Правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов ИКИ и Правилами обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности, информирует органы национальной безопасности Республики Казахстан.

15. В случаях, не терпящих отлагательств и могущих привести к совершению тяжких и особо тяжких преступлений, а также преступлений, подготавливаемых и совершаемых преступной группой, Председатель Комитета национальной безопасности Республики

Казахстан, его заместители или начальники территориальных органов Комитета национальной безопасности Республики Казахстан либо лица, их замещающие, вправе приостанавливать работу сетей и (или) средств связи, оказание услуг связи, доступ к интернет-ресурсам и (или) размещенной на них информации в интересах всех субъектов оперативно-розыскной деятельности с последующим уведомлением уполномоченного органа в области связи и Генеральной прокуратуры Республики Казахстан в течение 24-х часов.

16. При чрезвычайных ситуациях социального, природного и техногенного характера, введении чрезвычайного или военного положения уполномоченный орган по обеспечению информационной безопасности осуществляет координацию деятельности по управлению интернет-ресурсами и объектами ИКИ.

17. Меры реагирования на инциденты ИБ трансграничного характера согласовываются с уполномоченным органом по внешнеполитической деятельности и осуществляются в соответствии с международными договорами, ратифицированными Республикой Казахстан.

Параграф 4.2. Действия Оперативного штаба

18. В целях координации деятельности по реагированию на кризисные ситуации в сфере информационной безопасности на базе НКЦИБ создается оперативный штаб по реагированию на кризисные ситуации информационной безопасности (далее – Оперативный штаб).

19. До созыва Оперативного штаба НКЦИБ совместно с силами и средствами собственников и владельцев критически важных объектов ИКИ и объектов информатизации "электронного правительства" проводит мероприятия первичного реагирования на кризисную ситуацию с целью предотвращения распространения и минимизации ее последствий.

20. Руководителем Оперативного штаба является заместитель Председателя Комитета национальной безопасности, курирующий сферу информационной безопасности или исполняющий его обязанности. Заместителем руководителя Оперативного штаба является руководитель ведомства, уполномоченного органа в сфере обеспечения информационной безопасности, обеспечивающий реализацию государственной политики в сфере обеспечения информационной безопасности или исполняющий его обязанности.

21. По решению руководителя Оперативного штаба в его состав могут включаться представители государственных органов и иных организаций.

22. На основе первичного анализа кризисной ситуации информационной безопасности руководитель НКЦИБ предлагает руководителю Оперативного штаба решение о созыве Оперативного штаба для организации и реализации комплекса мер по ее предотвращению и локализации последствий инцидента информационной безопасности.

23. Основными задачами Оперативного штаба в кризисной ситуации являются:
определение порядка действий уполномоченных подразделений государственных органов и организаций по реагированию на кризисную ситуацию информационной безопасности;

внесение корректив в действия сил и средств уполномоченных подразделений государственных органов и организации по локализации и ликвидации кризисной ситуации информационной безопасности;

координация организационного и технического реагирования на кризисные ситуации в сфере информационной безопасности;

разработка и организация мероприятий по восстановлению функционирования информационно-коммуникационной инфраструктуры, работа которой была нарушена в период кризисной ситуации информационной безопасности;

организация служебных и технических расследований и разбирательств по установлению причин и условий возникновения кризисной ситуации информационной безопасности;

оповещение собственников и владельцев объектов информатизации об инцидентах информационной безопасности через средства массовой информации.