Приложение
к постановлению Правительства
Республики Казахстан
от « 14 » августа 2026 года
№ 725

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

Национальный антикризисный план реагирования на инциденты кибербезопасности

Глава 1. Общие положения

1. Национальный антикризисный план реагирования на инциденты кибербезопасности (далее – план) не распространяется на цифровые системы в защищенном исполнении, отнесенные к государственным секретам, цифровые объекты, содержащие сведения, составляющие государственные секреты, а также сети телекоммуникаций специального назначения и (или) президентской, правительственной и защищенной связи.

2. В настоящем плане используются следующие понятия:

1) объекты цифровой инфраструктуры – совокупность материальных, технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых объектов;

2) критически важные цифровые объекты – 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»;

3) система реагирования на инциденты кибербезопасности (далее – система) – совокупность сил и средств обеспечения кибербезопасности,

предназначенных для реализации общегосударственного комплекса мероприятий по защите цифровых ресурсов, цифровых систем и цифровой инфраструктуры от технологических сбоев или несанкционированного воздействия в результате компьютерных атак и ликвидации их последствий;

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

5) кризисная ситуация в сфере кибербезопасности – инцидент кибербезопасности, который привел или может привести к невозможности или ограничению предоставления государственных услуг, чрезвычайной ситуации социального и (или) техногенного характера или значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или жизнедеятельности населения, проживающего на соответствующей территории;

6) национальный координационный центр кибербезопасности (далее - НКЦКБ) – структурное подразделение акционерного общества «Государственная техническая служба»;

7) субъекты системы – государственные органы, уполномоченные на решение вопросов кибербезопасности или реагирования на инциденты кибербезопасности, НКЦКБ, оперативный штаб, владельцы цифровых объектов «цифрового правительства», владельцы критически важных цифровых объектов, центры обеспечения кибербезопасности, службы реагирования на инциденты кибербезопасности;

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

Глава 2. Профилактические мероприятия

3. В целях профилактики и недопущения инцидентов в сферах цифровизации и связи НКЦКБ на плановой основе проводит разъяснительные работы по инцидентам кибербезопасности, осуществляет сбор, анализ и обобщение информации отраслевых центров кибербезопасности и центров обеспечения кибербезопасности об инцидентах кибербезопасности на цифровых объектах «цифрового правительства» и критически важных цифровых объектах.

4. Центры обеспечения кибербезопасности в целях выявления и пресечения угроз кибербезопасности осуществляют мониторинг обеспечения кибербезопасности критически важных цифровых объектов, не относящихся к цифровым объектам «цифрового правительства».

5. Взаимодействие НКЦКБ с центрами обеспечения кибербезопасности при обмене информацией, необходимой для обеспечения кибербезопасности и

реагирования на инциденты кибербезопасности, определяется 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/НҚ (зарегистрирован в реестре государственной регистрации нормативных правовых актов под № 16886).

6. Субъекты системы для повышения уровня защищенности цифровых ресурсов, программного обеспечения, цифровых систем и поддерживающей их цифровой инфраструктуры руководствуются едиными требованиями в сферах цифровизации и обеспечения кибербезопасности, утвержденными постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832, а также иными нормативными правовыми актами, регламентирующими сферу кибербезопасности.

Глава 3. Действия собственников и владельцев критически важных цифровых объектов и цифровых объектов «цифрового правительства»

7. В целях обеспечения реагирования на инциденты кибербезопасности с уровнями критичности от 1 до 4 владельцы цифровых объектов «цифрового правительства», владельцы критически важных цифровых объектов, центры обеспечения кибербезопасности разрабатывают и утверждают планы реагирования, в которых предусматриваются меры по обработке угроз (рисков) кибербезопасности, 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 кибербезопасности;

2) сбору и анализу данных о состоянии кибербезопасности в цифровой инфраструктуре;

3) осуществлению взаимодействия с центрами обеспечения кибербезопасности и НКЦКБ;

4) поддерживающим мерам обеспечения непрерывности работы и устойчивости к внешним изменениям;

5) информированию заинтересованных субъектов системы по вопросам обнаруженных инцидентов кибербезопасности и их устранению;

6) порядку действий при ликвидации инцидентов кибербезопасности и их последствий, минимизации воздействия на цифровую инфраструктуру субъекта системы;

7) мерам сохранения цифровых следов инцидентов кибербезопасности (журналы, отчеты и формы);

8) установлению причин инцидентов кибербезопасности;

9) действиям, которые должны быть предприняты после инцидента кибербезопасности;

10) устранению причины инцидента кибербезопасности;

11) процедурам восстановления.

8. Владельцы цифровых объектов «цифрового правительства» и критически важных цифровых объектов направляют копию утвержденных планов реагирования на инциденты кибербезопасности в уполномоченный орган в сфере обеспечения кибербезопасности и НКЦКБ.

9. По вопросам инцидентов кибербезопасности собственники и владельцы критически важных цифровых объектов и цифровых объектов «цифрового правительства» взаимодействуют с НКЦКБ посредством круглосуточного call-центра 1400, платформы НКЦКБ, электронной почты incident@cert.gov.kz или официального сайта www.cert.gov.kz.

10. По решению владельцев цифровых объектов «цифрового правительства», критически важных цифровых объектов к реагированию на инциденты кибербезопасности привлекаются службы реагирования на инциденты кибербезопасности и (или) центры обеспечения кибербезопасности.

11. Владельцы цифровых объектов «цифрового правительства», критически важных цифровых объектов после завершения реагирования приступают к реализации предусмотренных планом мер по восстановлению системы, в том числе используя рекомендации уполномоченного органа в сфере обеспечения кибербезопасности и НКЦКБ.

12. В целях эффективного взаимодействия владельцы цифровых объектов «цифрового правительства», критически важных цифровых объектов определяют ответственных должностных лиц за обеспечение кибербезопасности.

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

Глава 4. Реагирование на инциденты кибербезопасности

Параграф 1. Действия уполномоченных органов по реагированию на инциденты кибербезопасности

13. НКЦКБ в случаях получения информации об инцидентах кибербезопасности на цифровых объектах в соответствии с 4-ым уровнем критичности инцидентов кибербезопасности информирует органы национальной безопасности Республики Казахстан.

14. 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 уполномоченных органов в областях связи, масс-медиа и Генеральной прокуратуры Республики Казахстан в течение двадцати четырех часов.

15. При чрезвычайных ситуациях социального, природного и техногенного характера, введении чрезвычайного или военного положения уполномоченный орган в сфере обеспечения кибербезопасности осуществляет координацию деятельности по управлению интернет-ресурсами и объектами цифровой инфраструктуры.

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

Параграф 2. Действия оперативного штаба

17. В целях координации деятельности по реагированию на кризисные ситуации в сфере кибербезопасности на базе НКЦКБ создается оперативный штаб по реагированию на кризисные ситуации кибербезопасности (далее – оперативный штаб).

18. До созыва оперативного штаба НКЦКБ в соответствии с подпунктом 1) пункта 1 статьи 7-7 Закона Республики Казахстан «О кибербезопасности» координирует работы по реагированию на кризисную ситуацию в сфере кибербезопасности, осуществляемые собственниками и владельцами критически важных цифровых объектов и цифровых объектов «цифрового правительства».

19. Руководителем оперативного штаба является заместитель Председателя Комитета национальной безопасности Республики Казахстан, курирующий сферу кибербезопасности или исполняющий его обязанности. Заместителем руководителя оперативного штаба является руководитель ведомства, уполномоченного органа в сфере обеспечения кибербезопасности, обеспечивающий реализацию государственной политики в сфере обеспечения кибербезопасности или исполняющий его обязанности.

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

21. На основе первичного анализа кризисной ситуации кибербезопасности руководитель НКЦКБ предлагает руководителю оперативного штаба решение о созыве Оперативного штаба для организации и реализации комплекса мер по ее предотвращению и локализации последствий инцидента кибербезопасности.

22. Основными задачами оперативного штаба в кризисной ситуации являются:

определение порядка действий уполномоченных подразделений государственных органов и организаций по реагированию на кризисную ситуацию кибербезопасности;

внесение корректировок в действия сил и средств уполномоченных подразделений государственных органов и организаций по локализации и ликвидации кризисной ситуации кибербезопасности;

координация организационного и технического реагирования на кризисные ситуации в сфере кибербезопасности;

разработка и организация мероприятий по восстановлению функционирования цифровой инфраструктуры, работа которой была нарушена в период кризисной ситуации кибербезопасности;

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

оповещение собственников и владельцев цифровых объектов об инцидентах кибербезопасности через средства массовой информации.