УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
14 февраля 2023 г. № 40

О кибербезопасности

В целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз п о с т а н о в л я ю:

1. Создать в Республике Беларусь национальную систему обеспечения кибербезопасности, элементами которой являются:

Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ);

Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности);

центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности);

оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (далее – авторизованный оператор электросвязи);

объекты информационной инфраструктуры государственных органов и иных организаций (далее – объекты информационной инфраструктуры);

сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в абзацах втором–пятом настоящего пункта.

2. Определить, что задачами национальной системы обеспечения кибербезопасности являются:

достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;

проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

прогнозирование ситуации в области обеспечения кибербезопасности.

3. Установить, что:

3.1. государственным органом, осуществляющим координацию деятельности других государственных органов и иных организаций по созданию и функционированию национальной системы обеспечения кибербезопасности, обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры, является ОАЦ, который:

определяет требования по кибербезопасности объектов информационной инфраструктуры;

устанавливает состав технических параметров киберинцидента, вырабатывает рекомендации по выявлению, предупреждению и исследованию кибератак, киберинцидентов, доводит их до сведения центров кибербезопасности;

определяет типовую структуру центров кибербезопасности и иные требования к ним, согласовывает назначение на должность руководителей таких центров, продление с ними трудового договора (контракта);

организует информационное взаимодействие элементов национальной системы обеспечения кибербезопасности, определяет порядок такого взаимодействия;

осуществляет сбор, обработку, накопление, систематизацию, хранение и поддержание в актуальном состоянии информации об элементах национальной системы обеспечения кибербезопасности;

информирует государственные органы и иные организации об угрозах в отношении принадлежащих им объектов информационной инфраструктуры и о необходимых мерах по нейтрализации данных угроз;

взаимодействует с иностранными и международными организациями по вопросам реагирования на киберинциденты, в том числе в рамках участия в форуме команд реагирования на компьютерные инциденты (FIRST), с уплатой взносов, связанных с таким участием;

выступает заказчиком государственных научно-технических и иных программ и проектов, организует проведение научно-исследовательских, опытно-конструкторских и иных работ в области обеспечения кибербезопасности;

принимает участие в выполнении иных мероприятий по созданию и развитию национальной системы обеспечения кибербезопасности;

вправе выносить обязательные для исполнения предписания:

операторам электросвязи – об ограничении или приостановлении оказания государственным органам и иным организациям услуг электросвязи в случае обнаружения киберинцидентов на объектах информационной инфраструктуры этих государственных органов и организаций;

государственным органам и иным организациям – об устранении выявленных нарушений положений настоящего Указа и иных актов законодательства, принятых в его развитие, а также требований по кибербезопасности объектов информационной инфраструктуры этих государственных органов и организаций;

3.2. для осуществления мероприятий по обнаружению признаков проведения кибератак на объекты информационной инфраструктуры, предупреждению и минимизации последствий этих кибератак, координации мероприятий по реагированию на киберинциденты в структуре ОАЦ создается Национальный центр кибербезопасности, который:

взаимодействует с центрами кибербезопасности, в том числе осуществляет сбор, обработку, анализ и обобщение информации, поступающей из этих центров, формирование и ведение общереспубликанской базы данных о киберинцидентах;

координирует и реализует мероприятия по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на объектах информационной инфраструктуры, реагированию на такие киберинциденты;

осуществляет автоматизированные сбор, обработку, накопление, систематизацию и хранение данных о кибербезопасности объектов информационной инфраструктуры, направленные на обнаружение, предотвращение и минимизацию последствий кибератак и вызванных ими киберинцидентов на указанных объектах, реагирование на такие киберинциденты;

оказывает методическую и практическую помощь государственным органам и иным организациям в вопросах обеспечения кибербезопасности принадлежащих им объектов информационной инфраструктуры;

проводит учения по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры, разрабатывает программы и методики проведения этих учений, сценарии реагирования на кибератаки;

организует проведение аналитических и научных исследований в области обеспечения кибербезопасности, при необходимости распространяет результаты таких исследований, в том числе в средствах массовой информации.

Для реализации функции реагирования на киберинциденты в составе Национального центра кибербезопасности создается и функционирует национальная команда реагирования на киберинциденты (CERT.BY), которая взаимодействует по данным вопросам:

на международном (межгосударственном) уровне – с форумом команд реагирования на компьютерные инциденты (FIRST);

на национальном уровне – с командами реагирования на киберинциденты центров кибербезопасности.

Порядок функционирования национальной команды реагирования на киберинциденты Национального центра кибербезопасности, команд реагирования на киберинциденты центров кибербезопасности определяется ОАЦ;

3.3. в рамках осуществления функций, возложенных на Национальный центр кибербезопасности, его уполномоченные лица вправе требовать от государственных органов и иных организаций:

представления документов (их копий) и (или) иной информации, в том числе технического характера, связанных с функционированием принадлежащих им объектов информационной инфраструктуры. Такие документы (их копии), иная информация должны быть представлены не позднее дня, следующего за днем предъявления требования об их представлении;

обеспечения беспрепятственного доступа в помещения и иные объекты (на территории), в которых размещены (функционируют) объекты информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование.

При обеспечении кибербезопасности объектов информационной инфраструктуры, в том числе реализации мероприятий по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты, уполномоченные лица центров кибербезопасности обладают правами, предусмотренными в части первой настоящего подпункта, в отношении объектов информационной инфраструктуры соответствующих государственных органов и иных организаций.

Уполномоченные лица организаций, оказывающих услуги по обеспечению кибербезопасности объектов информационной инфраструктуры, обладают правами, предусмотренными в части первой настоящего подпункта, если данные права определены в договоре на оказание услуг по обеспечению кибербезопасности;

3.4. перечень государственных органов и иных организаций, в том числе подчиненных (подотчетных) Президенту Республики Беларусь и Совету Министров Республики Беларусь, местных исполнительных и распорядительных органов, которые в сроки, устанавливаемые данным перечнем, создают центры кибербезопасности и (или) приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры, определяется Советом Министров Республики Беларусь по предложению ОАЦ и подлежит ежегодной актуализации.

Функции центров кибербезопасности государственных органов и иных организаций, включенных в перечень, указанный в части первой настоящего подпункта, могут возлагаться на подчиненные им (входящие в их состав, систему) юридические лица или структурные подразделения данных государственных органов и организаций.

В отношении государственных органов, обеспечение деятельности которых осуществляет Управление делами Президента Республики Беларусь, создание центров кибербезопасности и (или) приобретение услуг по обеспечению кибербезопасности у организаций, создавших такие центры, производятся Управлением делами Президента Республики Беларусь или уполномоченной им организацией;

3.5. владельцы критически важных объектов информатизации, указанные в приложении 1, а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечивают создание центров кибербезопасности в срок не позднее одного года со дня вступления в силу настоящего пункта;

3.6. помимо государственных органов и организаций, указанных в подпунктах 3.4 и 3.5 настоящего пункта, центры кибербезопасности могут создаваться организациями, имеющими лицензии на деятельность по технической и (или) криптографической защите информации в части составляющих данный вид деятельности работ по проектированию, созданию, аудиту систем информационной безопасности критически важных объектов информатизации;

3.7. до начала функционирования центры кибербезопасности подлежат аттестации, проводимой ОАЦ. В последующем аттестация проводится с периодичностью не реже одного раза в три года. Порядок проведения аттестации определяется ОАЦ;

3.8. центры кибербезопасности:

осуществляют автоматизированные сбор, обработку, накопление, систематизацию и хранение данных о кибербезопасности объектов информационной инфраструктуры, направленные на обнаружение, предотвращение и минимизацию последствий кибератак, а также мероприятия по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на указанных объектах, реагированию на такие киберинциденты;

проводят оценку степени защищенности объектов информационной инфраструктуры, мероприятия по установлению причин киберинцидентов, вызванных кибератаками на объекты информационной инфраструктуры;

осуществляют сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

информируют Национальный центр кибербезопасности о выявленных киберинцидентах не позднее одного часа с момента их выявления, а также представляют в указанный центр иные сведения, в том числе о результатах реагирования и ликвидации последствий киберинцидента в порядке, объеме и сроки, определяемые ОАЦ;

обеспечивают функционирование в своем составе команд реагирования на киберинциденты;

3.9. центры кибербезопасности организуют не реже одного раза в три года в республиканском унитарном предприятии «Национальный центр обмена трафиком» обучение своих работников, в обязанности которых входит обеспечение кибербезопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам кибербезопасности;

3.10. приобретение услуг по обеспечению кибербезопасности государственными органами и иными организациями осуществляется на основании договоров на оказание услуг с организациями, создавшими такие центры. Копия указанного договора направляется в ОАЦ в течение пяти рабочих дней со дня его заключения.

Центры кибербезопасности, функции которых возложены на структурные подразделения государственных органов и иных организаций, оказывают услуги по обеспечению кибербезопасности для государственных органов и иных организаций, в структуру которых они входят, без заключения договоров;

3.11. финансирование расходов по приобретению услуг по обеспечению кибербезопасности государственными органами и бюджетными организациями осуществляется за счет средств, ежегодно предусматриваемых в соответствующих бюджетах на их содержание, и иных источников, не запрещенных законодательством.

Оказание услуг по обеспечению кибербезопасности государственным органам и бюджетным организациям осуществляется с нормативом рентабельности не более пяти процентов к себестоимости для определения суммы прибыли, подлежащей включению в тарифы.

Расходы по созданию и функционированию центров кибербезопасности и (или) приобретению услуг по обеспечению кибербезопасности организациями, не являющимися государственными органами и бюджетными организациями, осуществляются за счет собственных средств этих организаций и иных источников, не запрещенных законодательством;

3.12. государственные органы и иные организации обеспечивают хранение информации о киберинцидентах, произошедших на принадлежащих им объектах информационной инфраструктуры, в течение не менее одного года;

3.13. функции авторизованного оператора электросвязи возлагаются на общество с ограниченной ответственностью «Белорусские облачные технологии».

Авторизованный оператор электросвязи обеспечивает оказание государственным органам и иным организациям услуг электросвязи, необходимых для организации

информационного взаимодействия этих органов и организаций с Национальным центром кибербезопасности и центрами кибербезопасности.

Указанные в части второй настоящего подпункта услуги государственным органам и иным организациям оказываются авторизованным оператором электросвязи на возмездной основе.

Оказание государственным органам и бюджетным организациям услуг электросвязи, необходимых для организации информационного взаимодействия этих органов и организаций с Национальным центром кибербезопасности и центрами кибербезопасности, осуществляется с нормативом рентабельности не более пяти процентов к себестоимости для определения суммы прибыли, подлежащей включению в тарифы.

Финансирование расходов по приобретению услуг электросвязи государственными органами и бюджетными организациями осуществляется за счет средств, ежегодно предусматриваемых в соответствующих бюджетах на их содержание, и иных источников, не запрещенных законодательством.

Расходы по приобретению услуг электросвязи организациями, не являющимися государственными органами и бюджетными организациями, осуществляются за счет средств этих организаций и иных источников, не запрещенных законодательством;

3.14. руководитель государственного органа и иной организации несет персональную ответственность за обеспечение кибербезопасности этого органа (организации);

3.15. руководители государственных органов и иных организаций, указанных в части первой подпункта 3.4 и подпункте 3.5 настоящего пункта, назначают одного из своих заместителей ответственным за организацию работы по обеспечению кибербезопасности этого органа (организации), в том числе за осуществление мероприятий по обнаружению, предотвращению и минимизации последствий кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты, если иное не предусмотрено частью второй настоящего подпункта.

Руководители государственных органов, обеспечение деятельности которых осуществляет Управление делами Президента Республики Беларусь, назначают ответственным за организацию работы, указанной в части первой настоящего подпункта, одного из своих заместителей либо иное уполномоченное лицо.

Права и обязанности заместителя руководителя (иного уполномоченного лица) государственного органа и иной организации, указанных в частях первой и второй настоящего подпункта, определяются руководителем этого органа (организации) с учетом рекомендаций ОАЦ.

4. Из абзаца пятого части первой пункта 13 Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» слова «, включая форум команд реагирования на компьютерные инциденты в качестве национального центра реагирования на компьютерные инциденты» исключить.

5. Для целей настоящего Указа применяются термины в значениях, определенных в приложении 2.

6. Совету Министров Республики Беларусь:

6.1. в двенадцатимесячный срок определить:

перечень государственных органов и иных организаций, которые создают центры кибербезопасности и (или) приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры;

перечень организаций, у которых государственные органы и иные государственные организации вправе приобретать услуги по обеспечению кибербезопасности с применением процедуры закупки из одного источника;

6.2. в шестимесячный срок принять иные меры по реализации настоящего Указа.

7. ОАЦ в шестимесячный срок обеспечить создание Национального центра кибербезопасности и принять иные меры по реализации настоящего Указа.

8. Настоящий Указ вступает в силу в следующем порядке:

пункты 1–5 – через шесть месяцев после официального опубликования настоящего Указа;

иные положения данного Указа – после его официального опубликования.

Президент Республики Беларусь **А.Лукашенко**

Приложение 1
к Указу Президента
Республики Беларусь
14.02.2023 № 40

ПЕРЕЧЕНЬ
владельцев критически важных объектов информатизации

1. Белорусское республиканское унитарное страховое предприятие «Белгосстрах».
2. Брестское республиканское унитарное предприятие электроэнергетики «Брестэнерго».
3. Витебское республиканское унитарное предприятие электроэнергетики «Витебскэнерго».
4. Гродненское республиканское унитарное предприятие электроэнергетики «Гродноэнерго».
5. Закрытое акционерное страховое общество «Промтрансинвест».
6. Минское республиканское унитарное предприятие электроэнергетики «Минскэнерго».
7. Могилевское республиканское унитарное предприятие электроэнергетики «Могилевэнерго».
8. Общество с ограниченной ответственностью «Белорусские облачные технологии».
9. Открытое акционерное общество «Банковский процессинговый центр».
10. Открытое акционерное общество «Белагропромбанк».
11. Открытое акционерное общество «Белорусский межбанковский расчетный центр».
12. Открытое акционерное общество «Газпром трансгаз Беларусь».
13. Открытое акционерное общество «Гомельтранснефть Дружба».
14. Открытое акционерное общество «Гродно Азот».
15. Открытое акционерное общество «Мозырский нефтеперерабатывающий завод».
16. Открытое акционерное общество «Нафтан».
17. Открытое акционерное общество «Небанковская кредитно-финансовая организация «Единое расчетное и информационное пространство».
18. Открытое акционерное общество «Сберегательный банк «Беларусбанк».
19. Открытое акционерное общество «Светлогорский целлюлозно-картонный комбинат».
20. Республиканское унитарное предприятие «Белорусская атомная электростанция».
21. Республиканское унитарное предприятие «Информационно-вычислительный центр Министерства финансов Республики Беларусь».
22. Республиканское унитарное предприятие «Национальный центр обмена трафиком».
23. Республиканское унитарное предприятие «Национальный центр электронных услуг».
24. Республиканское унитарное предприятие электросвязи «Белтелеком».

25. Совместное белорусско-российское открытое акционерное общество «Белгазпромбанк».

26. Совместное общество с ограниченной ответственностью «Мобильные ТелеСистемы».

27. Унитарное предприятие по оказанию услуг «А1».

Приложение 2
к Указу Президента
Республики Беларусь
14.02.2023 № 40

ПЕРЕЧЕНЬ
терминов и их определений

1. Информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.

2. Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

3. Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

4. Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности.

5. Объекты информационной инфраструктуры – критически важные объекты информатизации, информационные сети, информационные системы, информационные ресурсы и иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации, принадлежащие государственным органам и иным организациям на праве собственности, хозяйственного ведения, оперативного управления или на ином законном основании, за исключением объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты.

6. Хостинг – услуга по размещению информационного ресурса на сервере и обеспечению постоянного доступа к этому ресурсу в глобальной компьютерной сети Интернет.