ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
12 октября 2018 г. № 151

Об утверждении Положения об обеспечении безопасности критически важных объектов информатизации

На основании пункта 6 Положения об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденного Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение об обеспечении безопасности критически важных объектов информатизации.

2. Установить, что приведение в соответствие с настоящим приказом систем безопасности критически важных объектов информатизации, включенных в Государственный реестр критически важных объектов информатизации до вступления в силу данного приказа, не требуется.

3. Настоящий приказ вступает в силу с 30 октября 2018 г.

Начальник **А.Ю.Павлюченко**

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
12.10.2018 № 151

ПОЛОЖЕНИЕ
об обеспечении безопасности критически важных объектов информатизации

1. В настоящем Положении устанавливается порядок организации мероприятий по обеспечению безопасности критически важных объектов информатизации (далее – КВОИ), включая мероприятия по созданию системы безопасности КВОИ правового, организационного и технического характера, мониторингу угроз безопасности КВОИ и реагированию на такие угрозы.

2. Для целей настоящего Положения применяются термины и их определения в значениях, определенных Законом Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552), Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденным Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (Национальный реестр правовых актов Республики Беларусь, 2011 г., № 121, 1/13026), Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), техническими нормативными правовыми актами, а также следующие термины и их определения:

активы КВОИ – входящие в состав КВОИ технические, программные, программно-аппаратные средства (в том числе средства защиты информации), обрабатываемая

информация, системы управления информационными, производственными и (или) технологическими процессами;

владелец КВОИ – субъект, реализующий права владения, пользования и распоряжения КВОИ в соответствии с законодательством;

информационная безопасность КВОИ – состояние защищенности активов КВОИ от угроз безопасности КВОИ и рисков безопасности КВОИ;

риск безопасности КВОИ – вероятность реализации угроз безопасности активам КВОИ, которая может повлечь нарушение или прекращение их функционирования;

событие безопасности КВОИ – установленный факт реализации угроз безопасности КВОИ.

3. Для выполнения мероприятий по обеспечению безопасности КВОИ владельцем КВОИ назначается подразделение и (или) должностное лицо (работник), имеющее высшее образование в области технической и (или) криптографической защиты информации либо высшее или профессионально-техническое образование и прошедшее переподготовку или повышение квалификации по вопросам технической и (или) криптографической защиты информации в порядке, установленном законодательством (далее – служба безопасности (уполномоченный работник)).

4. Владельцы КВОИ разрабатывают и принимают (издают) локальные нормативные правовые акты, в которых определяются задачи и функции службы безопасности (уполномоченного работника) по вопросам обеспечения безопасности КВОИ, а также устанавливается порядок:

взаимодействия службы безопасности (уполномоченного работника) с иными работниками владельца КВОИ по вопросам обеспечения безопасности КВОИ;

согласования со службой безопасности (уполномоченным работником) приема, увольнения, перевода, перемещения работников, трудовые обязанности которых предусматривают эксплуатацию КВОИ, по вопросам обеспечения безопасности КВОИ;

проведения инструктажей, мероприятий по информированию и выработке практических навыков действий по обеспечению безопасности КВОИ;

защиты сведений, содержащихся в эксплуатационной документации на КВОИ, документации на систему безопасности КВОИ, иной информации, распространение и (или) предоставление которой ограничено, от ее разглашения или несанкционированного доступа к ней со стороны третьих лиц;

взаимодействия владельца КВОИ с иными юридическими и физическими лицами, в том числе при заключении и исполнении договоров, по вопросам обеспечения безопасности КВОИ.

5. Для обеспечения безопасности КВОИ создается система безопасности КВОИ, включающая комплекс мероприятий правового, организационного и технического характера, в том числе мероприятий по мониторингу угроз безопасности КВОИ и реагированию на такие угрозы.

6. Система безопасности КВОИ:

разрабатывается в целях оценки рисков безопасности КВОИ, обеспечения правильного выбора и последующей актуализации средств управления безопасностью КВОИ на всех стадиях его жизненного цикла, а также эффективности внутреннего контроля;

документально оформляется в виде формализованных правил и процедур управления безопасностью КВОИ.

7. В ходе создания системы безопасности КВОИ осуществляются:

7.1. определение главных и вспомогательных процессов основной деятельности владельца КВОИ;

7.2. определение внутренних (организационная структура, информационные системы, информационные потоки и процессы) и внешних аспектов (взаимосвязи с контрагентами и другое), оказывающих влияние на обеспечение безопасности КВОИ;

7.3. определение целей обеспечения безопасности КВОИ, совместимых с процессами деятельности владельца КВОИ и стратегией (концепцией, планом) развития;

7.4. разработка политики информационной безопасности, содержащей:

цели и процессы информационной безопасности;

перечень требований информационной безопасности и обязательства сотрудников по их выполнению;

организационную структуру системы безопасности;

обязательства по постоянному совершенствованию системы безопасности;

приоритетные направления информационной безопасности;

ссылки на нормы актов законодательства, в том числе технических нормативных правовых актов, а также на локальные нормативные правовые акты;

7.5. определение физических и логических границ области применения системы безопасности (формуляр, паспорт) с использованием структурной и логической схем КВОИ. Структурная схема отражает расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации. В логической схеме отражаются информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств;

7.6. инвентаризация (выявление и учет), а также определение степени важности (исходя из конфиденциальности, целостности и доступности) следующих активов КВОИ:

программно-аппаратных средств и физических устройств;

программного обеспечения (прикладного и системного);

средств защиты информации;

информационных систем и информационных сетей;

средств обработки информации (потоков информации), средств коммуникации;

информации, обрабатываемой на КВОИ, в том числе информации о настройках оборудования;

7.7. определение работников, ответственных за использование активов КВОИ;

7.8. определение угроз безопасности КВОИ;

7.9. классификация (категорирование) активов КВОИ по степени их значимости для основной деятельности владельца КВОИ;

7.10. классификация КВОИ в соответствии с СТБ 34.101.52-2016 «Информационные технологии. Методы и средства безопасности. Критически важные объекты информатизации. Классификация»;

7.11. разработка методологии оценки рисков безопасности КВОИ (методики оценки рисков). Владельцы КВОИ вправе разрабатывать методику оценки рисков в соответствии с СТБ 34.101.70-2016 «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах»;

7.12. оценка рисков безопасности КВОИ;

7.13. определение средств управления, необходимых для реализации выбранного варианта обработки рисков безопасности КВОИ (план обработки рисков);

7.14. согласование плана обработки рисков с руководством владельца КВОИ.

8. При создании системы безопасности КВОИ владельцы КВОИ вправе применять требования, предъявляемые к системе менеджмента информационной безопасности в соответствии с СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

9. По результатам создания системы безопасности владельцем КВОИ проводится оценка полноты и качества выполненных мероприятий на предмет того, что:

определена политика информационной безопасности;

определены приоритетные цели, задачи и направления деятельности организации;

распределены и согласованы обязанности работников и их ответственность по вопросам обеспечения безопасности КВОИ;

разработаны, приняты (изданы) локальные нормативные правовые акты, определяющие направления информационной безопасности КВОИ (политика информационной безопасности, формуляр (паспорт), реестр активов КВОИ, методика оценки рисков, план обработки рисков и другие), и доведены до сведения сотрудников, имеющих отношение к активам КВОИ, и третьих лиц, с которыми осуществляется взаимодействие;

определены условия конфиденциальности для обслуживающего персонала и третьих лиц;

представители службы безопасности (уполномоченный работник), должностные лица, ответственные за использование активов КВОИ, прошли обучение и осведомлены о правилах работы на КВОИ;

идентифицированы активы КВОИ, определены важные активы, необходимые для выполнения основных задач КВОИ;

контроль активов КВОИ осуществляется на всех этапах их жизненного цикла;

ведется учет и актуализированы схемы взаимодействия с внешними информационными системами;

обеспечено резервирование технических, программных, программно-аппаратных активов КВОИ, каналов связи (передачи данных), средств защиты информации;

определено максимальное допустимое время простоя КВОИ;

определены и задокументированы угрозы безопасности КВОИ, уязвимости его активов;

разработана методика оценки рисков;

разработан и согласован с руководством владельца КВОИ план обработки рисков. При этом должны быть определены критерии принятия рисков с учетом отраслевой принадлежности владельца КВОИ;

определены средства управления системой безопасности КВОИ и контролируется их функционирование и актуальность;

контролируется привлечение третьих лиц к разработке программного обеспечения;

доступ к активам КВОИ предоставляется только заранее определенному кругу лиц;

определен порядок физического доступа к активам КВОИ;

удаленный доступ к активам КВОИ допускается только в исключительных случаях (в целях выполнения технологических процессов на КВОИ, оперативного реагирования на возникновение угроз безопасности КВОИ) при условии обеспечения защиты передаваемых (получаемых) данных;

осуществляется контроль удаленного доступа к активам КВОИ, хранение сведений об изменении прав доступа и совершенных действиях;

определен порядок перемещения активов КВОИ через физические границы КВОИ;

контролируется целостность информационной сети (контроль за оборудованием и информационными потоками, настройками коммутационного оборудования и средств защиты информации);

задокументированы конфигурации активов КВОИ и осуществляется контроль изменений этих конфигураций;

внедрены процедуры резервного копирования и восстановления из резервных копий, резервные данные защищены в процессе их хранения;

определены правила уничтожения информации;

определен порядок получения разрешения службы безопасности (уполномоченного работника) на использование новых средств обработки информации;

ограничивается и контролируется порядок обращения с носителями информации;

силовые и коммуникационные сети, по которым передается информация или оказываются услуги, защищены от несанкционированного доступа и воздействия;

используются средства защиты информации от вредоносного программного обеспечения;

обеспечена защита информации, распространение и (или) предоставление которой ограничено, в соответствии с законодательством.

10. В целях проведения мониторинга угроз безопасности КВОИ и реагирования на эти угрозы владелец КВОИ:

осуществляет постоянный контроль состояния активов КВОИ в целях выявления потенциальных событий информационной безопасности КВОИ;

разрабатывает политику хранения журналов событий безопасности КВОИ, включая порядок и срок хранения журналов;

проводит анализ и оценку угроз безопасности КВОИ;

обеспечивает синхронизацию времени с единым источником;

разрабатывает план реагирования на события, которые могут стать причиной прерывания основных технологических процессов, оказания информационных услуг (далее – план реагирования), и проводит актуализацию плана реагирования не реже одного раз в год, а также в случае изменения нормативных правовых актов, структуры КВОИ, появления новых угроз безопасности КВОИ;

определяет периодичность проведения мероприятий по оповещению и отработке действий работников владельца КВОИ в случае реализации угроз безопасности КВОИ в соответствии с планом реагирования;

разрабатывает и внедряет методологию реагирования на события безопасности КВОИ, обеспечивающую реагирование в сроки, определенные эксплуатационной документацией на КВОИ и локальными нормативными правовыми актами, в целях исключения (снижения до приемлемого уровня) ущерба владельцу КВОИ. Методология реагирования на события безопасности КВОИ включает процедуры оповещения, реагирования и восстановления;

осуществляет регистрацию и обработку событий безопасности КВОИ;

разрабатывает план восстановления КВОИ, в котором учтены события безопасности КВОИ;

представляет в Оперативно-аналитический центр при Президенте Республики Беларусь сведения о событиях безопасности КВОИ;

осуществляет техническое обслуживание и ремонт активов КВОИ.

11. В целях определения соответствия функциональных характеристик КВОИ требованиям, установленным эксплуатационной документацией на КВОИ и техническими нормативными правовыми актами, осуществляется внутренний контроль.

Внутренний контроль осуществляется владельцем КВОИ не реже одного раза в год.

Результаты внутреннего контроля оформляются актом, который составляется в десятидневный срок с момента завершения мероприятий внутреннего контроля в двух экземплярах, один из которых в течение трех рабочих дней направляется в Оперативно-аналитический центр при Президенте Республики Беларусь.

12. Контроль проводится службой безопасности (уполномоченным работником) во взаимодействии с работниками, ответственными за использование активов КВОИ.

13. Внутренний контроль проводится при изменении условий, оказывающих влияние на функционирование КВОИ либо системы безопасности, и включает в себя следующие этапы:

анализ соответствия системы безопасности КВОИ требованиям, предусмотренным в пункте 9 настоящего Положения;

формирование замечаний (недостатков), выявленных в процессе контроля, и предложений по их устранению;

оформление акта по результатам контроля.