ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
25 июля 2023 г. № 130

О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40

На основании пункта 3 Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» ПРИКАЗЫВАЮ:

1. Утвердить:

Положение о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности (прилагается);

Положение о порядке функционирования национальной команды реагирования на киберинциденты Национального центра обеспечения кибербезопасности и реагирования на киберинциденты, команд реагирования на киберинциденты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (прилагается);

Положение о порядке проведения аттестации центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (прилагается).

2. Установить состав технических параметров киберинцидента согласно приложению 1.

3. Определить:

требования к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 2;

типовую структуру центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 3;

требования по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций согласно приложению 4.

4. Настоящий приказ вступает в силу с 17 августа 2023 г.

Начальник **А.Ю.Павлюченко**

Приложение 1
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

СОСТАВ
технических параметров киберинцидента

1. Технические параметры киберинцидента включают следующую информацию:

уровень киберинцидента и его наименование;

сетевые (IP) адреса версий 4 и (или) 6, подсети адресов объектов информационной инфраструктуры (при наличии);

доменные имена, связанные с объектами информационной инфраструктуры (при наличии);

уникальный идентификатор киберинцидента;

адреса электронной почты, URI-адреса объектов информационной инфраструктуры (при наличии);

сетевые (IP) адреса версий 4 и (или) 6, подсети адресов источников киберинцидента (при наличии);

доменные имена, связанные с источниками киберинцидента (при наличии);

адреса электронной почты, URI-адреса, связанные с источниками киберинцидента (при наличии);

вредоносные программы (при наличии);

идентификатор уязвимости с указанием системы классификации уязвимостей* (при наличии);

типы операционных систем, установленных на объектах информационной инфраструктуры;

дополнительные сведения, связанные с киберинцидентом (при наличии).

2. К киберинцидентам высокого уровня относятся:

внедрение и функционирование вредоносных программ на объектах информационной инфраструктуры;

несанкционированный доступ к объектам информационной инфраструктуры с использованием информационно-коммуникационных технологий;

использование объектов информационной инфраструктуры для осуществления кибератак и (или) распространения вредоносных программ;

прослушивание, захват, перенаправление сетевого трафика объектов информационной инфраструктуры;

рассылка незапрашиваемой информации (спама) с объектов информационной инфраструктуры;

эксплуатация уязвимостей на объектах информационной инфраструктуры;

прекращение функционирования объектов информационной инфраструктуры, вызванное кибератакой типа «отказ в обслуживании».

3. К киберинцидентам низкого уровня относятся:

попытка внедрения вредоносных программ на объектах информационной инфраструктуры;

проведение кибератаки типа «отказ в обслуживании», направленной на объекты информационной инфраструктуры, не вызвавшей негативных последствий;

попытка эксплуатации уязвимостей на объектах информационной инфраструктуры;

сканирование объектов информационной инфраструктуры в целях поиска уязвимостей;

попытка несанкционированного доступа к объектам информационной инфраструктуры;

прекращение функционирования объектов информационной инфраструктуры, не связанное с киберинцидентом высокого уровня;

попытка использования объектов информационной инфраструктуры для распространения вредоносных программ;

попытка проведения кибератаки на веб-приложения и иные сетевые протоколы и службы;

использование вычислительных мощностей объектов информационной инфраструктуры для проведения кибератак.

---

* Системы классификации уязвимостей – существующие международные или принятые в некоторых государствах перечни (реестры, базы данных) известных уязвимостей в безопасности (инфраструктуре) вычислительных систем.

Приложение 2
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ТРЕБОВАНИЯ
к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций

1. Центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности) должны обеспечивать:

1.1. наличие на праве собственности или ином законном основании необходимых для осуществления деятельности или оказания услуг по обеспечению кибербезопасности помещений, а также размещенных на территории Республики Беларусь:

средств выявления и реагирования на киберинциденты (система сбора и обработки событий информационной безопасности (SIEM); платформа управления информацией об угрозах (Threat Intelligence Platform); средство динамического анализа вредоносных программ типа «песочница»*; автоматизированная система взаимодействия);

средств аудита информационной безопасности и оценки эффективности защищенности (средств тестирования на проникновение) (сетевой сканер; сканер уязвимостей; сканер уязвимостей веб-приложений);

средств защиты информации, имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ);

* Наличие средства динамического анализа вредоносных программ типа «песочница» необязательно в случае заключения центром кибербезопасности со сторонней организацией или физическим лицом гражданско-правового договора на выполнение работ (оказание услуг) по анализу вредоносных программ.

1.2. соответствие типовой структуре центров кибербезопасности, определенной ОАЦ;

1.3. организацию информационного взаимодействия с Национальным центром обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности) с использованием автоматизированной системы взаимодействия;

1.4. наличие аттестованной системы защиты информации автоматизированной системы взаимодействия по классу типовых информационных систем 3-юл;

1.5. бесперебойное функционирование и восстановление работоспособности автоматизированной системы взаимодействия;

1.6. доступ к настройкам автоматизированной системы взаимодействия лиц, выполняющих функции по администрированию автоматизированных систем взаимодействия, из доверенного сетевого сегмента, определяемого центром кибербезопасности;

1.7. резервное копирование изменений конфигурационных файлов технических, программно-аппаратных и программных средств, в том числе средств защиты информации, восстановление этих файлов из резервных копий, а также хранение соответствующей информации не менее одного года;

1.8. контроль за соответствием состава технических, программно-аппаратных и программных средств, в том числе средств защиты информации, фактическому составу таких средств, контроль версий программного обеспечения;

1.9. синхронизацию системного времени от единого (общего) источника;

1.10. обновление технических, программно-аппаратных и программных средств, в том числе средств защиты информации, в течение месяца после выхода такого обновления;

1.11. централизованные сбор, обработку, накопление, систематизацию сведений о событиях информационной безопасности системы защиты информации автоматизированной системы взаимодействия и их хранение не менее одного года;

1.12. автоматизированные сбор, обработку, накопление, систематизацию и хранение сведений о событиях информационной безопасности и данных о киберинцидентах, поступающих от объектов информационной инфраструктуры, в круглосуточном режиме;

1.13. ежегодное планирование и проведение мероприятий по контролю эффективности защищенности системы защиты информации автоматизированной системы взаимодействия, а также объектов информационной инфраструктуры государственных органов и иных организаций;

1.14. устранение нарушений безопасности системы защиты информации автоматизированной системы взаимодействия. При отсутствии у центров кибербезопасности возможности устранения нарушений безопасности системы защиты информации автоматизированной системы взаимодействия собственными силами эти центры в течение одного часа с момента выявления таких нарушений информируют об этом Национальный центр кибербезопасности.

2. Руководитель центра кибербезопасности:

2.1. организует и контролирует проведение мероприятий по выявлению, предупреждению и исследованию киберинцидентов и кибератак на объектах информационной инфраструктуры, реагированию на киберинциденты;

2.2. организует автоматизированные сбор, обработку, накопление, систематизацию и хранение сведений о событиях информационной безопасности и данных о киберинцидентах, поступающих от объектов информационной инфраструктуры, мероприятия по выявлению и регистрации киберинцидентов;

2.3. организует мероприятия по оценке степени защищенности объектов информационной инфраструктуры, установлению причин киберинцидентов, вызванных кибератаками на объекты информационной инфраструктуры;

2.4. организует сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

2.5. обеспечивает подготовку ежегодных отчетов о состоянии кибербезопасности, защищенности объектов информационной инфраструктуры и их направление до 30 января года, следующего за отчетным, в Национальный центр кибербезопасности и лицу, ответственному за организацию работы по обеспечению кибербезопасности государственного органа и иной организации, в том числе за осуществление мероприятий по обнаружению, предотвращению и минимизации последствий кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты;

2.6. обеспечивает взаимодействие центра кибербезопасности с государственными органами и иными организациями по вопросам оказания услуг по обеспечению кибербезопасности;

2.7. организует защиту информации, обрабатываемой центром кибербезопасности, включая проведение практических занятий с работниками центра кибербезопасности по вопросам эксплуатации средств защиты информации;

2.8. осуществляет планирование мероприятий по обеспечению кибербезопасности объекта информационной инфраструктуры в случае возникновения нештатных ситуаций;

2.9. осуществляет контроль за выполнением работниками центра кибербезопасности требований нормативных правовых актов по вопросам обеспечения кибербезопасности и защиты информации;

2.10. разрабатывает предложения по вопросам совершенствования деятельности по обеспечению кибербезопасности объектов информационной инфраструктуры;

2.11. принимает участие в разработке проектов локальных правовых актов и других организационно-распорядительных документов по вопросам обеспечения кибербезопасности;

2.12. организует обучение и отработку действий работников центра кибербезопасности по обеспечению кибербезопасности объектов информационной инфраструктуры в случае возникновения нештатных ситуаций;

2.13. обеспечивает доведение до сведения работников центра кибербезопасности требований по обеспечению кибербезопасности объектов информационной инфраструктуры, в том числе предъявляемых к центрам кибербезопасности, а также положений организационно-распорядительных документов по вопросам обеспечения кибербезопасности указанных объектов в части, их касающейся;

2.14. осуществляет контроль осведомленности работников центра кибербезопасности об угрозах безопасности информации и уровня их знаний, практических навыков, необходимых для выполнения задач в соответствии с их обязанностями;

2.15. организует беспрепятственный доступ уполномоченных лиц Национального центра кибербезопасности в помещения и на 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;

2.16. оказывает практическую помощь в организации и проведении учений по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры;

2.17. должен знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

цели, задачи, способы, средства и специфика обеспечения кибербезопасности применительно к основным процессам функционирования государственного органа и иной организации;

направления стратегического развития кибербезопасности в государственном органе и иной организации;

возможные негативные последствия кибератак и вызванных ими киберинцидентов, а также способы обеспечения и поддержания необходимого уровня (состояния) кибербезопасности государственного органа и иной организации;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;

порядок реагирования на киберинциденты и ликвидации последствий киберинцидентов.

3. Лицо, выполняющее функции по автоматизированным сбору, обработке, накоплению, систематизации и хранению сведений о событиях информационной безопасности и данных о киберинцидентах:

3.1. осуществляет:

информационное взаимодействие с Национальным центром кибербезопасности;

в круглосуточном режиме автоматизированные сбор, обработку, накопление, систематизацию и хранение сведений о событиях информационной безопасности и данных о киберинцидентах, поступающих от объектов информационной инфраструктуры, а также выявление и регистрацию киберинцидентов;

3.2. определяет уровень киберинцидента, осуществляет сбор технических параметров киберинцидента;

3.3. координирует действия команды реагирования на киберинциденты центра кибербезопасности;

3.4. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

основные угрозы кибербезопасности, предпосылки их возникновения и возможные механизмы реализации этих угроз;

возможности и назначение средств защиты информации;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;

порядок реагирования на киберинциденты и ликвидации последствий кибератак.

4. Лицо, выполняющее функции по администрированию автоматизированной системы взаимодействия:

4.1. осуществляет:

анализ информации, предоставленной лицом, указанным в пункте 3 настоящих требований;

выявление и анализ событий информационной безопасности;

администрирование и настройку автоматизированной системы взаимодействия, участие в разработке и ведении базы правил корреляции событий информационной безопасности;

4.2. координирует действия лица, выполняющего функции по автоматизированным сбору, обработке, накоплению, систематизации и хранению сведений о событиях информационной безопасности и данных о киберинцидентах;

4.3. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

цели, задачи, способы, средства и специфика обеспечения кибербезопасности применительно к основным процессам функционирования государственного органа и иной организации;

основные угрозы кибербезопасности, предпосылки к их возникновению и возможные механизмы реализации этих угроз;

актуальные способы и средства проведения кибератак;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;

правила настройки и администрирования автоматизированной системы взаимодействия;

методика разработки правил корреляции событий информационной безопасности для автоматизированной системы взаимодействия.

5. Лицо, выполняющее функции по администрированию технических, программно-аппаратных и программных средств, в том числе средств защиты информации (член команды реагирования на киберинциденты центра кибербезопасности):

5.1. осуществляет:

реагирование на киберинциденты;

консультативную и техническую поддержку при реагировании на киберинциденты;

администрирование и настройку технических, программно-аппаратных, программных средств, в том числе средств защиты информации;

5.2. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

возможности и назначения технических, программно-аппаратных, программных средств, в том числе средств защиты информации;

правила администрирования и настройки технических, программно-аппаратных, программных средств, в том числе средств защиты информации;

состав, формат и типы записей журналов технических, программно-аппаратных, программных средств, в том числе средств защиты информации.

6. Лицо, ответственное за обеспечение кибербезопасности:

6.1. осуществляет:

анализ и обобщение информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

оценку эффективности защищенности объектов информационной инфраструктуры на предмет соответствия требованиям по кибербезопасности объектов информационной инфраструктуры;

6.2. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

цели, задачи, способы, средства и специфика обеспечения кибербезопасности применительно к основным процессам функционирования государственного органа и иной организации;

направления стратегического развития кибербезопасности в государственном органе и иной организации;

возможные негативные последствия кибератак и вызванных ими киберинцидентов, а также способы обеспечения и поддержания необходимого уровня (состояния) кибербезопасности государственного органа и иной организации;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности.

7. Лицо, выполняющее функции по анализу вредоносных программ:

7.1. осуществляет:

анализ данных о киберинцидентах с применением методов форензики (компьютерной криминалистики) и реверс-инжиниринга;

установление причин возникновения киберинцидентов с использованием вредоносных программ;

7.2. формирует рекомендации по устранению причин возникновения киберинцидентов с использованием вредоносных программ;

7.3. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

архитектура и принципы работы распространенных операционных систем;

принцип работы сетей передачи данных (протоколов) на всех уровнях модели взаимодействия открытых систем (OSI), основные способы сбора и анализа сетевого трафика;

механизмы работы систем постоянного хранения данных и оперативных запоминающих устройств;

принципы алгоритмизации и программирования;

способы компиляции и обфускации кода;

принципы статического и динамического анализа кода;

типы вредоносных программ, принципы их работы;

методы анализа вредоносных программ;

основные типы и форматы сведений, используемых в качестве индикаторов компрометации, порядок их формирования.

8. Лицо, выполняющее функции по оценке степени защищенности (тестирование на проникновение) объектов информационной инфраструктуры:

8.1. осуществляет:

оценку эффективности защищенности объектов информационной инфраструктуры и центра кибербезопасности на предмет наличия уязвимостей;

ручную и (или) автоматизированную проверку возможностей эксплуатации уязвимостей;

моделирование кибератак на объекты информационной инфраструктуры;

8.2. должно знать и иметь практические навыки по следующим вопросам:

основы построения информационных сетей, систем и ресурсов;

правила администрирования и настройки технических, программно-аппаратных, программных средств, в том числе средств защиты информации;

основные методы анализа защищенности веб-приложений, операционных систем;

методики проведения оценки эффективности защищенности объектов информационной инфраструктуры;

основные инструменты для проведения оценки эффективности защищенности объектов информационной инфраструктуры.

9. Лица, указанные в пунктах 2–8 настоящих требований, должны иметь высшее образование в области защиты информации либо высшее, или среднее специальное, или

профессионально-техническое образование и пройти в установленном порядке переподготовку или повышение квалификации по вопросам кибербезопасности.

10. Центры кибербезопасности до начала оказания услуг по обеспечению кибербезопасности обязаны:

10.1. разработать по каждому объекту информационной инфраструктуры регламент обеспечения кибербезопасности объекта информационной инфраструктуры (далее – регламент), который утверждается руководителем государственного органа или иной организации. В течение пяти рабочих дней со дня утверждения копия регламента направляется в Национальный центр кибербезопасности;

10.2. истребовать от государственного органа и иной организации информацию о назначении лица, ответственного 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.

11. В регламенте указывается следующая информация:

11.1. наименование объекта информационной инфраструктуры;

11.2. собственник (владелец) объекта информационной инфраструктуры (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей);

11.3. место нахождения объекта информационной инфраструктуры;

11.4. фамилия, собственное имя, отчество (если таковое имеется), должность, контактный номер телефона, адрес электронной почты лица, ответственного за организацию работы по обеспечению кибербезопасности государственного органа и иной организации, в том числе за осуществление мероприятий по обнаружению, предотвращению и минимизации последствий кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты;

11.5. контактный номер телефона, адрес электронной почты работника, ответственного за функционирование объектов информационной инфраструктуры, либо контактный номер телефона дежурной смены (при наличии);

11.6. порядок представления уполномоченным лицам центров кибербезопасности документов (их копий) и (или) иной информации, в том числе технического характера, связанных с функционированием объектов информационной инфраструктуры;

11.7. порядок обеспечения беспрепятственного доступа уполномоченных лиц центров кибербезопасности в помещения и на 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;

11.8. порядок автоматизированных сбора, обработки, накопления, систематизации и хранения сведений о событиях информационной безопасности и данных о киберинцидентах, выявления и регистрации киберинцидентов;

11.9. структурная схема объекта информационной инфраструктуры (расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программных, программно-аппаратных средств, в том числе средств защиты информации, автоматизированных рабочих мест администратора (оператора);

11.10. логическая схема объекта информационной инфраструктуры (информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств);

11.11. направление информационных потоков с указанием узлов сети, имеющих внешнее информационное взаимодействие;

11.12. список используемых доменных имен и IP-адресов, посредством которых осуществляется внешнее информационное взаимодействие.

В случае использования возможностей поставщиков интернет-услуг для размещения информационных систем (ресурсов) на основании заключаемых с ними гражданско-

правовых договоров в регламенте указывается полное наименование такого поставщика интернет-услуг, его регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей или учетный номер плательщика, место нахождения, контактный номер телефона, адрес электронной почты.

12. Договоры на оказание услуг по обеспечению кибербезопасности объектов информационной инфраструктуры должны содержать:

в качестве существенных условий – обязательства сторон по выполнению подпункта 10.1 пункта 10 и подпунктов 11.6–11.8 пункта 11 настоящих требований;

иные условия, обеспечивающие выполнение центрами кибербезопасности предъявляемых к ним требований в полном объеме.

Приложение 3
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ТИПОВАЯ СТРУКТУРА
центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций

1. Руководитель центра кибербезопасности.

2. Структурное подразделение, выполняющее функции по автоматизированным сбору, обработке, накоплению, систематизации и хранению сведений о событиях информационной безопасности и данных о киберинцидентах.

3. Структурное подразделение, выполняющее функции по администрированию автоматизированной системы взаимодействия.

4. Структурное подразделение, выполняющее функции команды реагирования на киберинциденты, а также функции по администрированию технических, программно-аппаратных и программных средств, в том числе средств защиты информации.

5. Структурное подразделение или лицо, ответственные за обеспечение кибербезопасности.

6. Структурное подразделение или лицо, выполняющие функции по анализу вредоносных программ.*

7. Структурное подразделение или лицо, выполняющие функции по оценке степени защищенности (тестирование на проникновение) объектов информационной инфраструктуры.*

* Для реализации функций, предусмотренных пунктами 6 и 7 настоящей типовой структуры, на основании гражданско-правовых договоров могут привлекаться сторонние организации или физические лица. В данном случае создание таких структурных подразделений или наличие в штате соответствующих лиц не требуется.

Приложение 4
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ТРЕБОВАНИЯ
по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций

1. К объектам информационной инфраструктуры предъявляются следующие требования по кибербезопасности:

1.1. использование технических, программно-аппаратных и программных средств, в том числе средств защиты информации, размещенных на территории Республики Беларусь;

1.2. применение средств защиты информации, прошедших подтверждение соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375;

1.3. наличие структурной и логической схем объектов информационной инфраструктуры, поддержание таких схем в актуальном состоянии;

1.4. определение порядка генерации и смены идентификационных и аутентификационных данных пользователей (паролей), обновления программного обеспечения, в том числе к средствам защиты информации;

1.5. изменение установленных по умолчанию идентификационных и аутентификационных данных (реквизитов доступа) к объектам информационной инфраструктуры, в том числе к средствам защиты информации, либо блокирование возможности их использования;

1.6. использование модели управления доступом (разграничения доступа) к объектам информационной инфраструктуры, в том числе к средствам защиты информации;

1.7. идентификация и аутентификация пользователей, своевременное блокирование (удаление) неиспользуемых идентификационных данных пользователей;

1.8. регламентированный доступ к настройкам (администрированию) объектов информационной инфраструктуры, в том числе средств защиты информации;

1.9. синхронизация системного времени от единого (общего) источника;

1.10. межсетевое экранирование при внешнем информационном взаимодействии по портам протоколов сетевого и транспортного уровней;

1.11. обнаружение и предотвращение вторжений при внешнем информационном взаимодействии;

1.12. защита от воздействия вредоносных программ;

1.13. централизованный сбор сведений о событиях информационной безопасности, а также хранение такой информации не менее одного года.

2. Государственный орган и иная организация вправе заключить гражданско-правовой договор на выполнение работ (оказание услуг), предусмотренных подпунктами 1.10, 1.11 и 1.13 пункта 1 настоящих требований, с поставщиками интернет-услуг и (или) организацией, оказывающими услуги по обеспечению кибербезопасности объектов информационной инфраструктуры.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ПОЛОЖЕНИЕ
о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности

1. Настоящим Положением определяется порядок информационного взаимодействия элементов национальной системы обеспечения кибербезопасности (далее – информационное взаимодействие).

2. Информационное взаимодействие осуществляется в целях:

сбора, обработки и хранения сведений о событиях информационной безопасности, поступающих от объектов информационной инфраструктуры;

регистрации киберинцидентов и хранения данных о них;

реализации мероприятий по выявлению, предупреждению и исследованию киберинцидентов и кибератак, реагированию на такие киберинциденты;

анализа информации о киберинцидентах и кибератаках, установления причин киберинцидентов;

предотвращения и минимизации последствий кибератак на объекты информационной инфраструктуры;

информирования государственных органов и иных организаций об угрозах в отношении принадлежащих им объектов информационной инфраструктуры и о необходимых мерах по нейтрализации данных угроз;

получения информации о средствах и способах проведения кибератак и о методах их предупреждения и обнаружения;

сбора, обработки, анализа и обобщения информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

обмена информацией по вопросам реагирования на киберинциденты, в том числе с иностранными и международными организациями.

3. Информационное взаимодействие осуществляется с использованием автоматизированных систем взаимодействия*.

В целях организации информационного взаимодействия и функционирования автоматизированных систем взаимодействия государственные органы и иные организации проводят организационно-технические мероприятия в соответствии с гражданско-правовыми договорами, заключаемыми с обществом с ограниченной ответственностью «Белорусские облачные технологии».

* Автоматизированная система взаимодействия – информационная система государственного органа и иной организации, предназначенная для сбора, обработки, накопления, систематизации и хранения событий информационной безопасности, регистрации киберинцидентов, а также направления и получения уведомлений (запросов) и иной информации в рамках информационного взаимодействия элементов национальной системы обеспечения кибербезопасности.

4. В случае проведения регламентных, профилактических и иных работ, которые могут повлечь приостановление функционирования автоматизированных систем взаимодействия, в качестве альтернативных способов информационного взаимодействия допускается использование:

автоматизированной системы государственной защищенной электронной почты ДСП для обмена информацией, распространение и (или) предоставление которой ограничено, за исключением сведений, составляющих государственные секреты;

системы межведомственного электронного документооборота государственных органов Республики Беларусь;

электронной почты, размещенной в национальном сегменте сети Интернет;

почтовой и телефонной связи.

Для повышения оперативности реагирования одновременно может использоваться несколько способов информационного взаимодействия.

5. При осуществлении информационного взаимодействия центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности) обеспечивают:

выявление возможных нарушений требований по кибербезопасности объектов информационной инфраструктуры;

корреляцию и объединение однородных сведений о событиях информационной безопасности (агрегацию), их фильтрацию и нормализацию;

корреляцию событий информационной безопасности с имеющимися индикаторами компрометации* в соответствии с правилами корреляции событий информационной безопасности;

анализ событий информационной безопасности и выявление связанных с ними киберинцидентов;

накопление индикаторов компрометации и их наполнение дополнительными сведениями, в том числе полученными в ходе реализации мероприятий по реагированию на киберинциденты;

оповещение в течение одного часа с момента выявления киберинцидента высокого уровня:

Национального центра обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности) с представлением сведений о результатах реагирования и ликвидации последствий киберинцидента;

лица, ответственного 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.

* Индикаторы компрометации – технические сведения, которые фактически или потенциально могут свидетельствовать о компрометации, попытках компрометации или иного вредоносного воздействия на объекты информационной инфраструктуры.

6. Правила корреляции событий информационной безопасности разрабатываются центрами кибербезопасности с учетом актуальных способов и средств проведения кибератак, в том числе информации, получаемой из Национального центра кибербезопасности, а также особенностей функционирования объектов информационной инфраструктуры, реализованных в ней бизнес-процессов и информационных потоков.

7. Сведения о событиях информационной безопасности, подлежащие сбору, обработке и хранению центром кибербезопасности, должны соответствовать перечню типов и записей событий информационной безопасности, установленному в приложении.

8. Выявленные киберинциденты регистрируются и данные о них хранятся в автоматизированной системе взаимодействия не менее одного года с момента их выявления.

Присвоенный автоматизированной системой взаимодействия регистрационный номер является уникальным идентификатором киберинцидента, обязательным для использования при информационном взаимодействии.

9. Получение центрами кибербезопасности информации о средствах и способах проведения кибератак и о методах их предупреждения и обнаружения осуществляется в соответствии с частью первой пункта 3 настоящего Положения.

10. Национальный центр кибербезопасности направляет центрам кибербезопасности информацию о средствах и способах проведения кибератак и о методах

их предупреждения и обнаружения с учетом особенностей функционирования объектов информационной инфраструктуры, реализованных в ней бизнес-процессов и информационных потоков.

11. Информация, поступающая из центров кибербезопасности, включается Национальным центром кибербезопасности в общереспубликанскую базу данных о киберинцидентах (далее – база данных) в целях:

накопления и хранения систематизированной информации о киберинцидентах, централизованного учета киберинцидентов;

оптимизации процесса корреляции данных о киберинцидентах, повышения качества и эффективности реагирования на киберинциденты, прогнозирования ситуации в области обеспечения кибербезопасности;

графической визуализации собранной информации для анализа и обобщения данных о киберинцидентах;

предоставления справочной информации о киберинцидентах.

12. В базу данных подлежат включению следующие данные о киберинцидентах:

дата и время возникновения киберинцидента, наименование и местонахождение объектов информационной инфраструктуры, на которых произошел киберинцидент;

причинно-следственная связь с другими киберинцидентами (при наличии);

фактическое состояние и характер мероприятий по реагированию на киберинциденты;

технические параметры киберинцидента;

назначение объектов информационной инфраструктуры, на которых произошел киберинцидент, тип обрабатываемых данных;

перечень взаимодействующих с объектами информационной инфраструктуры информационных систем и (или) ресурсов;

последствия киберинцидента.

13. Центры кибербезопасности направляют информацию в базу данных посредством автоматизированной системы взаимодействия.

14. Сведения из базы данных могут предоставляться государственным органам и иным организациям по их запросу, оформленному в письменной форме или в форме электронного документа.

В запросе указывается основание для получения сведений из базы данных со ссылкой на акт законодательства, запрашиваемые сведения, контактное лицо заявителя и его номер телефона.

Сведения из базы данных предоставляются в течение десяти рабочих дней со дня получения запроса.

В случае отсутствия в базе данных запрашиваемых сведений или невозможности их предоставления Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) информирует об этом государственный орган или иную организацию в течение десяти рабочих дней со дня получения запроса.

15. Обмен информацией с иностранными и международными организациями по вопросам реагирования на киберинциденты осуществляется ОАЦ, за исключением случаев, когда международным договором Республики Беларусь предусматривается возможность обмена такой информацией другими государственными органами и иными организациями.

В случае необходимости осуществления обмена информацией по вопросам реагирования на киберинциденты с иностранной или международной организацией государственный орган и иная организация направляют в ОАЦ письмо, содержащее обоснование необходимости обмена этой информацией, наименование, место нахождения иностранной или международной организации, а также иные необходимые для передачи информации сведения с приложением информации, составляющей предмет обмена.

В течение одного рабочего дня, следующего за днем получения письма, ОАЦ рассматривает информацию по вопросам реагирования на киберинциденты. В случае принятия решения о передаче этой информации в иностранную или международную

организацию ОАЦ незамедлительно направляет ее иностранной или международной организации, о чем одновременно информируется государственный орган или иная организация, направившие письмо.

В случае принятия ОАЦ решения об отказе в передаче информации по вопросам реагирования на киберинциденты иностранной или международной организации государственный орган и иная организация, направившие письмо, информируются об этом в течение одного рабочего дня, следующего за днем принятия решения, с указанием причин отказа.

При получении ответа от иностранной или международной организации ОАЦ в течение одного рабочего дня, следующего за днем его получения, направляет данный ответ государственному органу и иной организации, направившим письмо.

В случае получения государственным органом и иной организацией информации о киберинциденте, связанном с функционированием объектов информационной инфраструктуры, инициативно направленной иностранной или международной организацией, центр кибербезопасности направляет полученную информацию в ОАЦ не позднее одного рабочего дня, следующего за днем получения такой информации.

16. Информация, полученная ОАЦ от иностранной или международной организации, включается в базу данных.

Приложение
к Положению о порядке
информационного взаимодействия
элементов национальной системы
обеспечения кибербезопасности

ПЕРЕЧЕНЬ
типов и записей событий информационной безопасности

1. Для операционных систем:

запуск и (или) остановка системы;

запуск и (или) остановка процессов;

подключение съемных машинных носителей информации;

подключение иных периферийных устройств к портам ввода (вывода) (мобильные устройства, сетевые адаптеры, беспроводные модемы и иные);

установка и удаление программного обеспечения (изменение компонентов программного обеспечения);

аутентификация (вход и (или) выход) пользователей в операционной системе, успешные и неуспешные попытки аутентификации;

использование привилегированных учетных записей пользователей;

создание, удаление, модификация учетных записей пользователей;

неудавшиеся или отмененные действия пользователя и (или) процессы;

создание или изменение параметров заданий в планировщике задач;

установка, удаление, перезапуск, ошибка запуска службы и (или) сервиса;

изменение системной конфигурации, в том числе сетевых настроек и средств межсетевого экранирования;

изменение или попытки изменения настроек и средств управления защитой системы, в том числе антивирусного программного обеспечения, систем обнаружения и предотвращения вторжений;

контроль несанкционированных сетевых соединений, в том числе попыток несанкционированного удаленного доступа, создания общих сетевых ресурсов, использования нестандартных сетевых портов.

Запись события информационной безопасности операционных систем должна включать следующие поля:

дата и время возникновения события;

наименование учетной записи пользователя, которым инициировано событие;

IP-адрес хоста (устройства);

описание события информационной безопасности.

2. Для систем управления базами данных:

контроль сессий (успешные и (или) неуспешные авторизация, регистрация пользователей, попытки использования незарегистрированных учетных записей);

все действия пользователей, имеющих административные привилегии (включая команды «select», «create», «alter», «drop», «truncate», «rename», «insert», «update», «delete», «call (execute)», «lock»);

все действия пользователей, имеющих права на присвоение привилегий другим пользователям («grant», «revoke», «deny»).

Запись события информационной безопасности систем управления базами данных должна включать следующие поля:

дата и время возникновения события;

наименование учетной записи пользователя, которым инициировано событие;

IP-адрес хоста (устройства);

IP-адрес источника;

наименование устройства (при наличии);

описание события информационной безопасности.

3. Для телекоммуникационного оборудования:

запуск и (или) остановка системы;

изменение системной конфигурации;

создание, удаление, модификация локальных учетных записей пользователей;

использование привилегированных учетных записей пользователей;

подключение и (или) отключение устройства ввода (вывода);

неудавшиеся или отмененные действия пользователей;

включение, отключение, перезапуск сетевых интерфейсов.

Запись события информационной безопасности телекоммуникационного оборудования должна включать следующие поля:

наименование устройства;

наименования учетных записей пользователей;

IP-адрес хоста (устройства);

IP-адрес источника;

IP-адрес назначения;

описание события информационной безопасности.

С межсетевых экранов должна осуществляться запись информации о всех сетевых соединениях. Запись события информационной безопасности должна включать следующие поля:

дата и время возникновения события;

IP-адрес источника;

сетевой порт источника;

IP-адрес назначения;

сетевой порт назначения;

тип (код) протокола;

тип и код ICMP-пакета (при наличии возможности).

4. Для прикладного программного обеспечения:

аутентификация (вход и (или) выход) пользователей, успешные и неуспешные попытки аутентификации;

создание, копирование, перемещение, удаление, модификация учетных записей пользователей и конфигурационных файлов;

неудавшиеся или отмененные действия пользователей;

действия пользователей (доступ к объекту (данным), изменения объекта (данных), удаление объекта (данных).

Запись события информационной безопасности прикладного программного обеспечения должна включать следующие поля:

дата и время возникновения события;

наименование источника события (сервис и (или) служба);

наименования учетных записей пользователей;

IP-адрес источника;

IP-адрес хоста (устройств);

время начала операции;

время окончания операции;

описание события информационной безопасности.

5. Для средств защиты информации:

создание, копирование, перемещение, удаление, модификация учетных записей пользователей и конфигурационных файлов;

запуск и (или) остановка службы;

изменение системной конфигурации;

создание, удаление, модификация учетных записей пользователей.

Запись события информационной безопасности средств защиты информации должна включать в себя следующие поля:

дата и время возникновения события;

наименование источника события (сервис и (или) служба);

наименования учетных записей пользователей;

IP-адрес источника;

время начала и окончания операции;

описание события информационной безопасности.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ПОЛОЖЕНИЕ
о порядке функционирования национальной команды реагирования на киберинциденты Национального центра обеспечения кибербезопасности и реагирования на киберинциденты, команд реагирования на киберинциденты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций

1. Настоящим Положением регулируются отношения, связанные с порядком функционирования национальной команды реагирования на киберинциденты Национального центра обеспечения кибербезопасности и реагирования на киберинциденты (далее – национальная команда реагирования), команд реагирования на киберинциденты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – команды реагирования).

2. Национальная команда реагирования принимает участие в ликвидации последствий киберинцидентов высокого уровня, а также осуществляет координацию, методическое руководство проведением мероприятий по реагированию на киберинциденты.

Решение об участии национальной команды реагирования в ликвидации последствий киберинцидентов высокого уровня принимается руководителем Национального центра обеспечения кибербезопасности и реагирования

на киберинциденты (далее – Национальный центр кибербезопасности) по согласованию с начальником Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) или его уполномоченным заместителем.

В исключительных случаях начальником ОАЦ или его уполномоченным заместителем принимается решение об участии национальной команды реагирования в ликвидации последствий киберинцидентов низкого уровня.

3. Центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности) по каждому объекту информационной инфраструктуры разрабатывают план мероприятий по реагированию на киберинциденты (далее – план), который должен содержать:

перечень штатных единиц, входящих в состав команды реагирования, а также работников, ответственных за функционирование объектов информационной инфраструктуры, с указанием обязанностей этих лиц по выполнению предусмотренных планом мероприятий;

события (условия), при наступлении которых реализуются мероприятия, предусмотренные планом;

мероприятия, проводимые в ходе реагирования на киберинциденты, очередность выполняемых командами реагирования действий, а также время, отводимое на их реализацию, исходя из особенностей функционирования объектов информационной инфраструктуры, реализованных в ней бизнес-процессов и информационных потоков, иных факторов, способных оказать влияние на реализацию этих мероприятий.

План утверждается руководителем центра кибербезопасности, и в течение пяти рабочих дней со дня утверждения его копия направляется в Национальный центр кибербезопасности и лицу, ответственному 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 (далее – уполномоченное лицо).

4. До принятия мер по реагированию на киберинциденты и ликвидации их последствий Национальный центр кибербезопасности, а также центры кибербезопасности определяют:

персональный состав команд реагирования, их задачи и функции;

состав лиц, привлекаемых помимо команд реагирования для реализации мероприятий по реагированию на киберинциденты;

перечень средств, необходимых для проведения мероприятий по реагированию на киберинциденты;

очередность объектов информационной инфраструктуры, в отношении которых будут проводиться мероприятия по реагированию на киберинциденты;

перечень мероприятий по восстановлению функционирования объектов информационной инфраструктуры.

Возможность и порядок использования средств, необходимых для проведения мероприятий по реагированию на киберинциденты, с учетом особенностей функционирования объекта информационной инфраструктуры согласовывается с уполномоченным лицом.

5. В ходе реагирования на киберинциденты в целях установления причин киберинцидентов и принятия мер по ликвидации их последствий национальная команда реагирования и команды реагирования:

на основании имеющихся в автоматизированных системах взаимодействия индикаторов компрометации определяют перечень объектов информационной инфраструктуры, вовлеченных в киберинцидент;

осуществляют анализ сведений о событиях информационной безопасности, связанных с киберинцидентами (включая определение очередности реагирования на них), а также иной необходимой информации;

проводят опрос работников, ответственных за функционирование объектов информационной инфраструктуры государственных органов и иных организаций, на предмет установления их причастности к киберинциденту;

выявляют источники кибератак и вызванных ими киберинцидентов, проводят оценку возможностей (потенциала) внешних и внутренних нарушителей;

определяют возможные способы возникновения киберинцидентов;

осуществляют анализ возможных уязвимостей объектов информационной инфраструктуры и технических, программно-аппаратных и программных средств, в том числе средств защиты информации;

принимают меры по обеспечению сохранности информации, содержащейся на машинных носителях информации, записей сетевого трафика посредством создания их копий;

по результатам ликвидации киберинцидентов формируют дополнительные индикаторы компрометации и составляют отчет о результатах реагирования на киберинциденты.

6. В целях предотвращения и минимизации последствий киберинцидентов мероприятия по реагированию могут включать принятие мер, направленных на ограничение функционирования объектов информационной инфраструктуры.

7. Меры по восстановлению функционирования объектов информационной инфраструктуры и проверке их работоспособности принимаются после завершения мероприятий по ликвидации последствий киберинцидентов.

При выявлении на объекте информационной инфраструктуры киберинцидентов высокого уровня до ликвидации их последствий не допускается:

изменять конфигурационные файлы технических, программно-аппаратных и программных средств, в том числе средств защиты информации;

осуществлять поиск и удаление экземпляров вредоносных программ;

проводить обновление программного обеспечения;

выполнять мероприятия по восстановлению информации из резервных копий;

выполнять иные действия, которые могут привести к уничтожению индикаторов компрометации.

8. Отчеты о результатах реагирования на киберинциденты формируются в автоматизированных системах взаимодействия с указанием:

перечня объектов информационной инфраструктуры, вовлеченных в киберинцидент;

технических параметров киберинцидента;

описания выявленных индикаторов компрометации и причин киберинцидентов;

информации о восстановлении объекта информационной инфраструктуры (полное, частичное, невозможно восстановить, восстановление не требуется);

перечня предпринятых командами реагирования и работниками, ответственными за функционирование объектов информационной инфраструктуры, действий, направленных на ликвидацию последствий киберинцидентов;

описания выявленных нарушений требований по кибербезопасности и рекомендаций по их устранению.

9. Отчеты о результатах реагирования на киберинциденты направляются в Национальный центр кибербезопасности и уполномоченному лицу в порядке и сроки, предусмотренные Положением о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности, утвержденным приказом, утвердившим настоящее Положение.

10. Центры кибербезопасности проводят тренировки по вопросам обеспечения кибербезопасности объектов информационной инфраструктуры на случай возникновения нештатных ситуаций с оценкой эффективности таких тренировок.

Периодичность проведения тренировок определяется руководителями центров кибербезопасности с учетом особенностей функционирования объектов информационной инфраструктуры, реализованных в ней бизнес-процессов и информационных потоков.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 № 130

ПОЛОЖЕНИЕ
о порядке проведения аттестации центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций

1. Настоящим Положением определяется порядок проведения Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) аттестации центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности).

2. Аттестация предусматривает комплексную процедуру оценки центров кибербезопасности, осуществляемую до начала их функционирования, в результате которой документально подтверждается соответствие центров кибербезопасности предъявляемым к ним требованиям.

3. Решение о проведении аттестации принимается начальником ОАЦ в форме приказа, в соответствии с которым создается комиссия для проведения аттестации (далее – комиссия) и определяется ее персональный состав.

4. Председатель комиссии определяет перечень вопросов, подлежащих рассмотрению при проведении аттестации.

5. Для проведения аттестации собственник (владелец) объекта информационной инфраструктуры или организация, создавшие центр кибербезопасности (далее – заявители), направляют в ОАЦ заявление о проведении аттестации центра кибербезопасности (далее – заявление) по форме согласно приложению.

К заявлению прилагаются:

сведения о работниках центра кибербезопасности (фамилия, собственное имя, отчество (если таковое имеется), идентификационный номер (при наличии), дата и номер приказа о приеме на работу, информация об образовании, переподготовке, повышении квалификации), в том числе копии документов, подтверждающих данные сведения;

информация о наличии на праве собственности или ином законном основании помещений, а также размещенных на территории Республики Беларусь технических, программно-аппаратных и программных средств, в том числе средств защиты информации, необходимых для осуществления деятельности или оказания услуг по обеспечению кибербезопасности.

6. Заявление с прилагаемыми к нему документами (сведениями) может быть подано в ОАЦ лично заявителем (его представителем) либо направлено посредством системы межведомственного электронного документооборота государственных органов Республики Беларусь (далее – СМДО) или почтовой связи заказным письмом с заказным уведомлением о получении.

Личное представление указанных в части первой настоящего пункта документов (сведений) осуществляется заявителем (его представителем) с одновременным предъявлением:

документа, удостоверяющего личность, и документа, подтверждающего полномочия руководителя (приказ о назначении на должность руководителя, или выписка из решения общего собрания, правления либо иного органа управления юридического лица, или трудовой договор (контракт), или гражданско-правовой договор), – руководителем заявителя;

документа, удостоверяющего личность, и доверенности или иного документа, подтверждающего полномочия на совершение юридически значимых действий от имени заявителя, – уполномоченным представителем заявителя.

7. При нахождении заявителя в процессе ликвидации, а также в случаях указания в заявлении не всех сведений либо представления не всех документов, предусмотренных настоящим Положением, в приеме заявления к рассмотрению может быть отказано. Мотивированный отказ в приеме заявления не позднее пяти рабочих дней, следующих за днем поступления его в ОАЦ, направляется вместе с этим заявлением и прилагаемыми к нему документами (сведениями) заявителю посредством СМДО или почтовой связи заказным письмом с заказным уведомлением о получении.

8. Срок проведения аттестации не может превышать 25 рабочих дней со дня поступления заявления и прилагаемых к нему документов (сведений).

9. Мероприятия по аттестации могут проводиться по месту нахождения центра кибербезопасности или помещений, которые будут использоваться для оказания услуг по обеспечению кибербезопасности. В этом случае заявитель извещается о дате начала проведения мероприятий по аттестации не позднее чем за три рабочих дня до начала их проведения. Уведомление о дате начала проведения выездных мероприятий по аттестации должно содержать сведения о дате начала их проведения, сроках их проведения, а также о вопросах, подлежащих рассмотрению при проведении аттестации.

Перед началом проведения указанных мероприятий уполномоченные на их проведение лица обязаны предъявить служебное удостоверение.

10. Аттестация включает изучение и анализ имеющихся в ОАЦ, представленных заявителем и полученных при необходимости у иных государственных органов и других организаций документов (сведений), подтверждающих соответствие центра кибербезопасности предъявляемым к нему требованиям, а также путем установления:

факта наличия на праве собственности или ином законном основании помещений, технических, программно-аппаратных и программных средств, в том числе средств защиты информации, необходимых для осуществления деятельности или оказания услуг по обеспечению кибербезопасности;

соответствия структуры центра кибербезопасности типовой структуре таких центров (изучение штатного расписания, трудовых книжек, должностных инструкций, распорядительных документов (приказов) и т.п.);

факта наличия у работников центра кибербезопасности необходимого образования, переподготовки, повышения квалификации;

объективной возможности оказания услуг по обеспечению кибербезопасности силами имеющейся штатной численности центра кибербезопасности.

11. По результатам проведения аттестации комиссией составляется заключение о соответствии или несоответствии центра кибербезопасности предъявляемым к нему требованиям. Заключение подписывается председателем и членами комиссии и учитывается при принятии ОАЦ решений, указанных в части первой пункта 12 настоящего Положения.

12. По результатам проведения аттестации ОАЦ принимает одно из следующих решений:

об аттестации центра кибербезопасности;

об отказе в аттестации центра кибербезопасности.

Решения, указанные в части первой настоящего пункта, оформляются приказами ОАЦ.

Уведомление о принятом решении в течение трех рабочих дней со дня его принятия направляется заявителю посредством СМДО или почтовой связи заказным письмом с заказным уведомлением о получении.

13. Решение об отказе в аттестации центра кибербезопасности принимается в случае:

наличия в заявлении и прилагаемых к нему документах (сведениях) фактов недостоверности сведений, необходимых (имеющих значение) для принятия решения об аттестации центра кибербезопасности;

наличия заключения комиссии о несоответствии центра кибербезопасности предъявляемым к нему требованиям, составленного по результатам проведенной аттестации;

отказа заявителя в письменной форме от проведения аттестации либо непредставления заявителем в процессе проведения аттестации информации или документов, подтверждающих соответствие центра кибербезопасности предъявляемым к нему требованиям.

14. После устранения несоответствий, повлекших отказ в аттестации центра кибербезопасности, заявитель вправе вновь обратиться в ОАЦ с заявлением, но не ранее десяти рабочих дней со дня принятия ОАЦ соответствующего решения.

15. Центры кибербезопасности подлежат переаттестации не реже одного раза в три года, а также в случаях:

наличия в ОАЦ сведений, в том числе полученных от государственного органа или иной организации, свидетельствующих о несоответствии центров кибербезопасности предъявляемым к ним требованиям или невыполнении возложенных на них задач;

изменения центрами кибербезопасности организационных, программных и (или) программно-технических решений, необходимых для оказания услуг по обеспечению кибербезопасности;

изменения требований, предъявляемых к центрам кибербезопасности.

О проведении переаттестации ОАЦ письменно уведомляет собственника (владельца) объекта информационной инфраструктуры или организацию, создавшую центр кибербезопасности, не менее чем за три рабочих дня до ее проведения.

Переаттестация проводится в течение 15 рабочих дней со дня направления уведомления о ее проведении в порядке, установленном для проведения аттестации.

16. В случае планируемого прекращения оказания услуг по обеспечению кибербезопасности центр кибербезопасности не менее чем за 20 календарных дней до предполагаемой даты прекращения оказания этих услуг уведомляет ОАЦ, а также государственные органы и иные организации, которым оказываются данные услуги.

17. Принятое ОАЦ по результатам проведения аттестации решение может быть обжаловано заявителем в судебном порядке.

Приложение
к Положению о порядке
проведения аттестации центров
обеспечения кибербезопасности
и реагирования на киберинциденты
объектов информационной
инфраструктуры государственных
органов и иных организаций

Форма

Угловой штамп или бланк заявителя

Оперативно-аналитический центр
при Президенте Республики Беларусь

ЗАЯВЛЕНИЕ
о проведении аттестации центра кибербезопасности

_____
(полное наименование заявителя, место нахождения)

регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей _____,
номер телефона _____, адрес электронной почты _____,
в лице _____
(должность, фамилия, собственное имя, отчество (если таковое имеется)

_____
руководителя заявителя (его представителя)
подтверждает, что:

_____,
(наименование центра кибербезопасности,

_____,
место нахождения)

соответствует требованиям, предъявляемым к ним;
заявитель не находится в процессе ликвидации.
Прошу провести аттестацию указанного центра кибербезопасности.

Приложение: _____
(наименование прилагаемых документов)

Руководитель заявителя
(его представитель) _____ _____
(подпись) (инициалы, фамилия)

____._____.20___