Зарегистрировано в Национальном реестре правовых актов
Республики Беларусь 26 июля 2023 г. N 7/5425

ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
25 июля 2023 г. N 130

О МЕРАХ ПО РЕАЛИЗАЦИИ УКАЗА ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ОТ 14 ФЕВРАЛЯ 2023 Г. N 40

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

На основании абзацев второго - пятого подпункта 3.1, части третьей подпункта 3.2, подпункта 3.7 и абзаца пятого подпункта 3.8 пункта 3 Указа Президента Республики Беларусь от 14 февраля 2023 г. N 40 "О кибербезопасности" ПРИКАЗЫВАЮ:
(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

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.

3-1. Для целей настоящего приказа термины используются в значениях, определенных в приложении 5.
(п. 3-1 введен приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

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 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

СОСТАВ
ТЕХНИЧЕСКИХ ПАРАМЕТРОВ КИБЕРИНЦИДЕНТА
(в ред. приказа Оперативно-аналитического центра при Президенте
Республики Беларусь от 27.05.2026 N 98)

1. Технические параметры киберинцидента включают следующую информацию:

уровень киберинцидента (высокий, средний, низкий) и его наименование;

тип кибератаки, повлекшей возникновение киберинцидента, и иные сведения, связанные с кибератакой;

сетевые (IP) адреса версий 4 и (или) 6, подсети этих адресов, порты транспортного уровня, связанные с источниками проведения кибератаки и объектами информационной инфраструктуры, на которых возник киберинцидент;

доменные имена, уникальные идентификаторы ресурсов (URI), связанные с источниками проведения кибератаки и объектами информационной инфраструктуры, на которых возник киберинцидент;

уникальный идентификатор киберинцидента в системе обработки сведений о киберинцидентах;

адреса электронной почты, связанные с источниками проведения кибератаки и объектами информационной инфраструктуры, на которых возник киберинцидент;

сведения о вредоносном программном обеспечении;

идентификатор уязвимости с указанием системы классификации уязвимостей;

сведения об операционных системах, связанных с источниками проведения кибератаки и объектами информационной инфраструктуры, на которых возник киберинцидент;

временные метки недопустимых событий кибербезопасности;

хэш-суммы файлов вредоносного программного обеспечения;

причины возникновения киберинцидента (при их установлении);

иные сведения, связанные с киберинцидентом (при их наличии).

2. К киберинцидентам высокого уровня относятся вызванные кибератакой:

2.1. нарушение на срок более трех часов или прекращение функционирования:

критически важных объектов информатизации, а также объектов информатизации, подлежащих отнесению к критически важным объектам информатизации;

объектов информационной инфраструктуры государственных органов и иных организаций, включенных в определяемый Советом Министров Республики Беларусь перечень государственных органов и иных организаций, которые создают центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры и (или) приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры;

2.2. нарушение конфиденциальности:

служебной информации ограниченного распространения;

персональных данных, обрабатываемых объектами информационной инфраструктуры, посредством которых осуществляется:

трансграничная передача специальных персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, за исключением случаев, предусмотренных абзацами пятым - седьмым пункта 1 статьи 9 Закона Республики Беларусь от 7 мая 2021 г. N 99-З "О защите персональных данных";

обработка биометрических и (или) генетических персональных данных;

обработка персональных данных более 100 тыс. физических лиц;

обработка персональных данных более 10 тыс. физических лиц, не достигших возраста 16 лет;

2.3. нарушение целостности или доступности информации, обрабатываемой объектами информационной инфраструктуры, повлекшее распространение недостоверной общественно значимой информации.

3. К киберинцидентам среднего уровня относятся вызванные кибератакой:

нарушение на срок более трех часов или прекращение функционирования объектов информационной инфраструктуры, за исключением случаев, предусмотренных в подпункте 2.1 пункта 2 настоящего приложения;

нарушение конфиденциальности, целостности или доступности информации, обрабатываемой объектами информационной инфраструктуры, за исключением случаев, предусмотренных в подпунктах 2.2 и 2.3 пункта 2 настоящего приложения;

несанкционированный доступ к объектам информационной инфраструктуры, не повлекший нарушения конфиденциальности, целостности или доступности обрабатываемой такими объектами информации.

4. К киберинцидентам низкого уровня относятся иные события, за исключением указанных в пунктах 2 и 3 настоящего приложения, которые фактически или потенциально угрожают конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляют собой нарушение (угрозу нарушения) политики безопасности.

5. Кибератаки классифицируются по следующим типам:

5.1. в зависимости от направленности кибератаки:

массовые кибератаки;

целенаправленные кибератаки;

5.2. в зависимости от субъекта, проводящего кибератаку:

кибератаки внешних нарушителей;

кибератаки внутренних нарушителей;

5.3. в зависимости от характера кибератаки:

внедрение вредоносного программного обеспечения;

использование методов социальной инженерии;

атаки на сеть и протоколы (например, атаки типов "отказ в обслуживании" (DoS) и "распределенный отказ в обслуживании" (DDoS), атака посредника, DNS/ARP-спуфинг);

несанкционированный доступ (например, в результате хищения реквизитов доступа, подбора паролей, обхода аутентификации);

эксплуатация уязвимостей, ошибок конфигурации (например, SQL-инъекция, межсайтовый скриптинг (XSS), повышение привилегий, переполнение буфера);

злоупотребление правами;

атаки через цепочку поставок (компрометация подрядчика);

использование съемных носителей информации с вредоносным программным обеспечением;

иные целенаправленные воздействия 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.

Приложение 2
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130

(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ТРЕБОВАНИЯ
К ЦЕНТРАМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ИНЫХ ОРГАНИЗАЦИЙ

(в ред. приказа Оперативно-аналитического центра при Президенте
Республики Беларусь от 27.05.2026 N 98)

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:

помещений;

системы сбора, обработки и хранения событий кибербезопасности;

платформы управления информацией о киберугрозах;

системы обработки сведений о киберинцидентах;

средств динамического анализа вредоносного программного обеспечения <*>;

средств для оценки эффективности защищенности объектов информационной инфраструктуры от кибератак (далее - средства для оценки эффективности защищенности) <*>;

<*> Наличие средств динамического анализа вредоносного программного обеспечения и средств для оценки эффективности защищенности в обязательном порядке обеспечивают центры кибербезопасности, планирующие оказывать услуги по обеспечению кибербезопасности.

1.2. наличие в штате работников в соответствии с типовой структурой центров кибербезопасности. При этом не допускается:

возложение обязанностей лиц, указанных в типовой структуре, на другие структурные подразделения государственных органов и иных организаций, в которых созданы центры кибербезопасности;

совмещение обязанностей лиц, относящихся к разным позициям типовой структуры, за исключением случаев временного отсутствия соответствующих лиц;

1.3. достаточность теоретических и практических знаний (навыков) работников центров кибербезопасности;

1.4. организацию информационного взаимодействия с Национальным центром обеспечения кибербезопасности и реагирования на киберинциденты (далее - Национальный центр кибербезопасности);

1.5. автоматизированные сбор и обработку в круглосуточном режиме событий кибербезопасности, поступающих от объектов информационной инфраструктуры, в том числе выявление недопустимых событий кибербезопасности;

1.6. функционирование в своем составе команды реагирования на киберинциденты (далее - команда реагирования);

1.7. наличие аттестованной собственными силами (без привлечения третьих лиц) системы защиты информации объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности <*>, по классу типовых информационных систем 3-юл;

<*> Такой объект информационной инфраструктуры должен быть расположен на территории Республики Беларусь, а для центров кибербезопасности, планирующих оказывать услуги по обеспечению кибербезопасности, - дополнительно должен

функционировать отдельно от других объектов информационной инфраструктуры государственных органов и иных организаций.

1.8. доступ к настройкам активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации для лиц, ответственных за администрирование этих активов и средств, из доверенных сетевых сегментов, определяемых центром кибербезопасности;

1.9. резервное копирование изменений конфигурационных файлов активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации, контроль работоспособности резервных копий, а также хранение соответствующих копий не менее одного года в выделенном для этого сетевом сегменте;

1.10. контроль за составом активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации, в том числе контроль версий программного обеспечения;

1.11. обновление программного обеспечения, относящегося к активам объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемым на этом объекте средствам защиты информации, в течение месяца, а для обновлений, устраняющих критические уязвимости, - в течение трех рабочих дней после выхода таких обновлений (за исключением случаев, когда возможность таких обновлений ограничена производителем, а также случаев, влекущих нарушение или прекращение функционирования названных активов и средств);

1.12. синхронизацию системного времени для активов объектов информационной инфраструктуры государственных органов и иных организаций, включая объект информационной инфраструктуры, эксплуатируемый центром кибербезопасности, и применяемых на этих объектах средств защиты информации от единого источника времени, используя данные республиканского унитарного предприятия "Белорусский государственный институт метрологии";

1.13. эксплуатацию средства анализа вредоносного программного обеспечения с использованием выделенного для этих целей внешнего сетевого (IP) адреса, отличного от внешних сетевых (IP) адресов активов объектов информационной инфраструктуры государственных органов и иных организаций и применяемых на этих объектах средств защиты информации.

2. Помимо требований, определенных в пункте 1 настоящего приложения, аттестованные центры кибербезопасности обеспечивают:

2.1. проведение в государственных органах и иных организациях на плановой основе, но не реже одного раза в год аудита кибербезопасности, который включает следующие этапы:

2.1.1. подготовительный этап, реализуемый по согласованию с собственником (владельцем) объекта информационной инфраструктуры, на котором определяются сроки проведения аудита кибербезопасности, порядок и сроки представления отчета о результатах его проведения;

2.1.2. основной этап, на котором проводятся мероприятия, направленные на получение информации о деятельности государственного органа и иной организации по обеспечению кибербезопасности и установление степени соответствия выполнения требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций, требований по защите информации, распространение и (или) предоставление которой ограничено, а также обрабатываемой на критически важных объектах информатизации.

При проведении основного этапа:

осуществляется ознакомление с локальными правовыми актами и другими организационно-распорядительными документами по вопросам обеспечения кибербезопасности и защиты информации, структурными и логическими схемами объектов информационной инфраструктуры;

устанавливается фактический состав информационной инфраструктуры государственных органов и иных организаций, а также соответствие:

фактического состава активов объекта информационной инфраструктуры, средств

защиты информации - структурным и логическим схемам объектов информационной инфраструктуры;

фактической реализации организационных и технических мер по выполнению требований, указанных в части первой настоящего подпункта, - локальным правовым актам и другим организационно-распорядительным документам государственных органов и иных организаций.

При проведении основного этапа могут опрашиваться работники собственника (владельца) объекта информационной инфраструктуры по вопросам, связанным с проведением аудита кибербезопасности, а также проводиться иные мероприятия, направленные на достижение цели аудита кибербезопасности;

2.1.3. завершающий этап, на котором формируется отчет о результатах проведения аудита кибербезопасности.

Отчет о результатах проведения аудита кибербезопасности составляется в произвольной форме и должен содержать сведения о результатах проведения соответствующих мероприятий, выявленные несоответствия требованиям, указанным в части первой подпункта 2.1.2 настоящего пункта, и рекомендации по их устранению. Отчет о результатах проведения аудита кибербезопасности дополнительно может содержать иные сведения;

2.2. проведение в государственных органах и иных организациях на плановой основе, но не реже одного раза в год оценки эффективности защищенности объектов информационной инфраструктуры от кибератак (далее - оценка эффективности защищенности). Оценка эффективности защищенности проводится в отношении каждого объекта информационной инфраструктуры и включает следующие этапы:

2.2.1. подготовительный этап, реализуемый по согласованию с собственником (владельцем) объекта информационной инфраструктуры, на котором:

определяется перечень объектов информационной инфраструктуры, подлежащих оценке эффективности защищенности, фиксируются границы для проведения оценки (целевые сетевые (IP) адреса, подсети, доменные имена, физические границы объектов информационной инфраструктуры, активы этих объектов, средства защиты информации, которые не подлежат оценке);

определяется методология и способы проведения мероприятий по оценке эффективности защищенности (методы "черный ящик", "серый ящик", "белый ящик"; оценка внешнего периметра (инструментальное сканирование; тестирование на проникновение, в том числе эксплуатация выявленных уязвимостей, ошибок конфигурации); тестирование веб-приложений и мобильных приложений; моделирование кибератак, в том числе с использованием методов социальной инженерии);

в зависимости от выбранного метода тестирования фиксируется перечень исходных сведений об объектах информационной инфраструктуры, в отношении которых проводится оценка эффективности защищенности, активах этих объектов, средствах защиты информации (реквизиты доступа, дополнительные сетевые (IP) адреса, адреса электронной почты, исходные коды приложений, сведения о конфигурации), определяются исходные позиции для проведения мероприятий по оценке эффективности защищенности (со стороны внешнего контура, из внутреннего периметра информационной инфраструктуры, использование удаленного подключения, сторонних объектов информационной инфраструктуры);

фиксируются ограничения, определяется перечень активов объекта информационной инфраструктуры, нарушение функционирования которых недопустимо, ситуации, при которых требуется досрочное прекращение проведения мероприятий по оценке эффективности защищенности, формируется перечень мер, достаточных для обеспечения непрерывной работы и восстановления работоспособности объекта информационной инфраструктуры на период проведения этих мероприятий;

определяются сроки проведения мероприятий по оценке эффективности защищенности, порядок и сроки представления отчета об оценке эффективности защищенности;

2.2.2. основной этап, на котором актуализируются сведения, необходимые для проведения оценки эффективности защищенности, а также проводятся активные мероприятия по оценке эффективности защищенности.

Актуализация сведений, необходимых для проведения оценки эффективности защищенности, осуществляется, в частности, посредством:

поиска информации из открытых источников без непосредственного взаимодействия с объектами информационной инфраструктуры, подлежащими оценке эффективности защищенности;

инструментального сканирования объектов информационной инфраструктуры, подлежащих оценке эффективности защищенности, на предмет определения типов и версий программного обеспечения, наличия уязвимостей, ошибок конфигурации. При этом применяются различные средства оценки эффективности защищенности (сетевые сканеры, сканеры уязвимостей, сканеры уязвимостей веб-приложений).

Активные мероприятия по оценке эффективности защищенности, в частности, включают:

моделирование и проведение потенциально возможных кибератак;

тестирование на проникновение, в том числе путем ручного и автоматизированного тестирования, эксплуатации выявленных уязвимостей, ошибок конфигурации, получения доступа к объектам информационной инфраструктуры и обрабатываемой такими объектами информации.

В рамках проведения активных мероприятий по оценке эффективности защищенности по согласованию с собственником (владельцем) объекта информационной инфраструктуры могут применяться методы социальной инженерии, а также осуществляться оценка эффективности защищенности беспроводных сетей передачи информации, физической безопасности помещений и иных объектов (территорий), в которых размещены (функционируют) объекты информационной инфраструктуры;

2.2.3. завершающий этап, на котором:

обобщаются и анализируются сведения, полученные в ходе предыдущих этапов;

объект информационной инфраструктуры приводится в исходное состояние;

формируется отчет об оценке эффективности защищенности, который должен содержать сведения о результатах проведения соответствующих мероприятий, выявленных проблемных аспектах защищенности объекта информационной инфраструктуры и рекомендации по их устранению, описание выявленных уязвимостей с указанием их критичности и результатов эксплуатации этих уязвимостей, сведения о полученном уровне привилегии. Отчет об оценке эффективности защищенности дополнительно может содержать иные сведения.

Рекомендации по оформлению отчета об оценке эффективности защищенности размещаются на официальном интернет-сайте Оперативно-аналитического центра при Президенте Республики Беларусь (далее - ОАЦ);

2.3. участие в учениях по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры, проводимых Национальным центром кибербезопасности.

3. Для операционных систем, систем управления базами данных, телекоммуникационного оборудования, прикладного программного обеспечения и средств защиты информации устанавливаются следующие события кибербезопасности, подлежащие сбору, обработке и хранению:

3.1. для операционных систем:

запуск и (или) остановка системы и (или) процессов;

подключение съемных носителей информации и иных периферийных устройств к портам ввода (вывода) (мобильные устройства, сетевые адаптеры, беспроводные модемы и другое);

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, ошибки 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;

ведение журналов DNS-запросов.

Запуск процессов должен осуществляться с записью аудита команд и (или) скриптов.

Запись события кибербезопасности операционных систем должна включать следующие поля:

дата и время возникновения события;

наименование учетной записи пользователя, которым инициировано событие;

сетевой (IP) адрес хоста (устройства);

описание события кибербезопасности;

3.2. для систем управления базами данных:

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

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

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

Запись события кибербезопасности систем управления базами данных должна включать следующие поля:

дата и время возникновения события;

наименование учетной записи пользователя, которым инициировано событие;

сетевой (IP) адрес хоста (устройства);

сетевой (IP) адрес источника;

наименование устройства;

описание события кибербезопасности;

3.3. 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 кибербезопасности телекоммуникационного оборудования должна включать следующие поля:

наименование устройства;

наименования учетных записей пользователей;

сетевой (IP) адрес хоста (устройства);

сетевой (IP) адрес источника;

сетевой (IP) адрес назначения;

описание события кибербезопасности;

3.4. 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;

действия пользователей по доступу к объекту (данным), изменению или удалению объекта (данных), а также неудавшиеся или отмененные действия пользователей.

Запись события кибербезопасности прикладного программного обеспечения должна включать следующие поля:

дата и время возникновения события;

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

наименования учетных записей пользователей;

сетевой (IP) адрес источника;
сетевой (IP) адрес хоста (устройства);
время начала операции;
время окончания операции;
описание события кибербезопасности;
3.5. для средств защиты информации (кроме межсетевых экранов):
запуск и (или) остановка компонентов (служб) средств защиты информации;
изменение системной конфигурации и конфигурационных файлов средств защиты информации;
события, связанные с регистрацией нарушений правил безопасности, обнаружением угроз;
создание, удаление, модификация учетных записей пользователей;
аутентификация (вход и (или) выход) пользователей, успешные и неуспешные попытки аутентификации.
Запись события кибербезопасности средств защиты информации (кроме межсетевых экранов) должна включать следующие поля:
дата и время возникновения события;
наименование источника события (сервис и (или) служба);
наименования учетных записей пользователей;
сетевой (IP) адрес источника;
время начала и окончания операции;
описание события кибербезопасности.
Для межсетевых экранов должна осуществляться запись сведений о всех сетевых соединениях. Запись события кибербезопасности межсетевых экранов должна включать следующие поля:
дата и время возникновения события;
сетевой (IP) адрес источника;
сетевой порт источника;
сетевой (IP) адрес назначения;
сетевой порт назначения;
тип (код) протокола;
тип и код ICMP-пакета.
4. Руководитель центра кибербезопасности:
4.1. обеспечивает взаимодействие центра кибербезопасности с Национальным центром кибербезопасности, организует беспрепятственный доступ уполномоченных лиц Национального центра кибербезопасности в помещения и на иные объекты (территории), в которых размещены (функционируют) объекты информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование;
4.2. организует обучение работников центра кибербезопасности;
4.3. должен знать:
основы законодательства, регулирующего отношения в области обеспечения кибербезопасности, в сфере технической и криптографической защиты информации;
основы построения и функционирования объектов информационной инфраструктуры;
цели, задачи, способы, средства и специфику обеспечения кибербезопасности применительно к основным процессам функционирования государственного органа и иной организации;
возможные направления развития кибербезопасности в государственном органе и иной организации на краткосрочный и долгосрочный периоды;
возможные негативные последствия кибератак и вызванных ими киберинцидентов;
возможности и назначение средств защиты информации;
порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;
порядок реагирования на киберинциденты.
5. Для согласования назначения на должность руководителя центра кибербезопасности, продления с ним трудового договора (контракта) в ОАЦ посредством

системы межведомственного электронного документооборота государственных органов Республики Беларусь или автоматизированной системы государственной защищенной электронной почты ДСП направляется письмо, в котором указываются фамилия, собственное имя, отчество (если таковое имеется) кандидата на указанную должность (руководителя центра кибербезопасности), сведения о его трудовой деятельности, информация об образовании, личный номер телефона, адрес электронной почты. По решению государственного органа и иной организации в письме дополнительно могут быть указаны иные сведения.

При рассмотрении вопроса о согласовании назначения на должность руководителя центра кибербезопасности, продления с ним трудового договора (контракта) с кандидатом на эту должность (руководителем центра кибербезопасности) уполномоченными должностными лицами Национального центра кибербезопасности, как правило, проводится собеседование.

Письмо о согласовании продления трудового договора (контракта) с руководителем центра кибербезопасности направляется в ОАЦ не позднее чем за два месяца до истечения срока его действия.

Согласование назначения на должность руководителя центра кибербезопасности, продления с ним трудового договора (контракта) осуществляется в течение 20 календарных дней со дня поступления в ОАЦ письма, указанного в части первой настоящего пункта.

6. Лицо, ответственное за проведение аудита кибербезопасности:

6.1. осуществляет подготовку локальных правовых актов и других организационно-распорядительных документов по вопросам деятельности центра кибербезопасности, обеспечивает их поддержание в актуальном состоянии;

6.2. проводит аудит кибербезопасности;

6.3. анализирует и обобщает информацию о кибербезопасности объектов информационной инфраструктуры, включая информацию о причинах возникновения киберинцидентов;

6.4. формирует предложения по совершенствованию функционирования центра кибербезопасности, требований по кибербезопасности;

6.5. принимает участие в подготовке проектов договоров об оказании услуг по обеспечению кибербезопасности и осуществлении контроля за их исполнением;

6.6. в случае отсутствия руководителя центра кибербезопасности исполняет его обязанности по обеспечению взаимодействия с Национальным центром кибербезопасности <*>;

<*> Кроме случаев, когда структура центра кибербезопасности включает должность заместителя руководителя центра кибербезопасности.

6.7. должно знать:

законодательство, регулирующее отношения в области обеспечения кибербезопасности, в сфере технической и криптографической защиты информации;

основы функционирования объектов информационной инфраструктуры;

возможности и назначение средств защиты информации;

возможные негативные последствия кибератак и вызванных ими киберинцидентов.

7. Лицо, ответственное за сбор и обработку событий кибербезопасности:

7.1. координирует работу лиц, ответственных за выявление киберинцидентов;

7.2. осуществляет:

анализ событий кибербезопасности, поступающих от объектов информационной инфраструктуры, выявление киберинцидентов;

настройку системы сбора, обработки и хранения событий кибербезопасности;

ведение базы правил корреляции событий кибербезопасности, их разработку с учетом актуальных способов и средств проведения кибератак, особенностей функционирования объектов информационной инфраструктуры и рекомендаций Национального центра кибербезопасности;

нормализацию, агрегацию и корреляцию событий кибербезопасности, в том числе с учетом имеющихся индикаторов компрометации;

сбор, обработку и хранение индикаторов компрометации;

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

основы построения и функционирования объектов информационной инфраструктуры;

техники и тактики проведения кибератак;

актуальные способы и средства проведения кибератак;

возможности и назначение средств защиты информации;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;

настройка системы сбора, обработки и хранения событий кибербезопасности;

методика разработки правил корреляции событий кибербезопасности для системы сбора, обработки и хранения событий кибербезопасности.

8. Лицо, ответственное за выявление киберинцидентов:

8.1. обеспечивает обработку событий кибербезопасности, поступающих от объектов информационной инфраструктуры, выявление и регистрацию киберинцидентов, в том числе в автоматизированной системе информационного взаимодействия;

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

8.3. осуществляет информационное обеспечение команды реагирования;

8.4. эксплуатирует систему сбора, обработки и хранения событий кибербезопасности, систему обработки сведений о киберинцидентах;

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

основы построения и функционирования объектов информационной инфраструктуры;

техники и тактики проведения кибератак;

возможности и назначение средств защиты информации;

порядок информационного взаимодействия при решении вопросов обеспечения кибербезопасности;

основы эксплуатации системы сбора, обработки и хранения событий кибербезопасности, системы обработки сведений о киберинцидентах.

9. Лицо, ответственное за администрирование активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации:

9.1. осуществляет:

администрирование активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации;

настройку активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации, за исключением системы сбора, обработки и хранения событий кибербезопасности, средств динамического анализа вредоносного программного обеспечения и средств для оценки эффективности защищенности (при наличии в штате лиц, ответственных за проведение анализа вредоносного программного обеспечения и оценки эффективности защищенности);

сбор, обработку и хранение индикаторов компрометации;

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

основы построения и функционирования объектов информационной инфраструктуры;

возможности и назначение активов объектов информационной инфраструктуры, средств защиты информации;

администрирование и настройка активов объектов информационной инфраструктуры, средств защиты информации;

состав, формат и типы записей журналов активов объектов информационной инфраструктуры, средств защиты информации.

10. Лицо, ответственное за проведение анализа вредоносного программного обеспечения:

10.1. анализирует сведения о киберинцидентах с применением методов форензики

(компьютерной криминалистики) и реверс-инжиниринга;

10.2. устанавливает причины возникновения киберинцидентов, связанных с внедрением вредоносного программного обеспечения;

10.3. осуществляет настройку и эксплуатацию средств динамического анализа вредоносного программного обеспечения, выявление индикаторов компрометации;

10.4. формирует рекомендации по устранению причин возникновения киберинцидентов, связанных с внедрением вредоносного программного обеспечения;

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

основы построения и функционирования объектов информационной инфраструктуры;

архитектура и принципы работы операционных систем;

принципы работы сетей передачи данных (протоколов) на всех уровнях модели взаимодействия открытых систем, 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 вредоносного программного обеспечения, принципы его работы;

методы анализа вредоносного программного обеспечения;

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

11. Лицо, ответственное за проведение оценки эффективности защищенности:

11.1. проводит оценку эффективности защищенности;

11.2. осуществляет настройку и эксплуатацию средств для оценки эффективности защищенности;

11.3. взаимодействует с государственными органами и иными организациями по вопросам проведения оценки эффективности защищенности;

11.4. обобщает и анализирует сведения, полученные при проведении оценки эффективности защищенности, формирует предложения по повышению эффективности защищенности объектов информационной инфраструктуры от кибератак;

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

основы построения и функционирования объектов информационной инфраструктуры;

администрирование и настройка активов объектов информационной инфраструктуры, средств защиты информации;

методики, тактики и техники проведения мероприятий по оценке эффективности защищенности.

12. Центры кибербезопасности после их аттестации (в случае оказания услуг по обеспечению кибербезопасности - после заключения договора на оказание этих услуг) обязаны:

провести аудит кибербезопасности;

разработать по каждому объекту информационной инфраструктуры регламент обеспечения кибербезопасности (далее - регламент) и план мероприятий по реагированию на киберинциденты (далее - план), поддерживать данные документы в актуальном состоянии. Регламент и план утверждаются руководителем государственного органа и иной организации или его уполномоченным заместителем.

13. Регламент должен содержать:

13.1. наименование объекта информационной инфраструктуры;

13.2. сведения о собственнике (владельце) объекта информационной инфраструктуры (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей);

13.3. сведения о поставщике интернет-услуг (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей) в случае приобретения услуги хостинга официального интернет-сайта и электронной почты;

13.4. фамилию, собственное имя, отчество (если таковое имеется), должность служащего, 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;

13.5. контактные номера телефонов, адреса электронной почты работников, ответственных за функционирование объекта информационной инфраструктуры, защиту информации, обрабатываемой этим объектом, иных лиц, привлекаемых для обеспечения функционирования объекта информационной инфраструктуры, защиты информации, обрабатываемой этим объектом, либо контактный номер телефона дежурной смены (при наличии);

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

13.7. порядок обеспечения доступа уполномоченных лиц центра кибербезопасности к объекту информационной инфраструктуры;

13.8. порядок автоматизированных сбора, обработки, хранения событий кибербезопасности и данных о киберинцидентах, выявления и регистрации киберинцидентов;

13.9. перечень недопустимых событий кибербезопасности;

13.10. структурную и логическую схемы объекта информационной инфраструктуры.

Структурная схема объекта информационной инфраструктуры должна содержать:

места размещения физических устройств, относящихся к активам объекта информационной инфраструктуры, средств защиты информации, название каждого устройства согласно его системному имени (серийный номер - для неуправляемого устройства), названия физических интерфейсов устройства;

физические линии связи с указанием их типа (витая пара, волоконно-оптический кабель или другое), идентификаторы виртуальных локальных вычислительных сетей (VLAN ID);

физические границы объекта информационной инфраструктуры.

К структурной схеме объекта информационной инфраструктуры прилагаются:

сведения о назначении линий связи (передача данных или управление активами объекта информационной инфраструктуры, средствами защиты информации);

перечень виртуальных локальных вычислительных сетей (VLAN) с указанием их идентификаторов (VLAN ID), названий виртуальных локальных вычислительных сетей (VLAN Name), сетевой (IP) адресации, используемой в виртуальных локальных вычислительных сетях (VLAN);

перечень телекоммуникационного оборудования с указанием производителя оборудования, его модели, системного имени (серийного номера - для неуправляемого устройства), сетевого (IP) адреса управления устройством, места размещения (помещение, номер стойки, место в стойке или другое).

Логическая схема объекта информационной инфраструктуры должна содержать:

направления внутренних и внешних информационных потоков;

логические границы объекта информационной инфраструктуры.

К логической схеме объекта информационной инфраструктуры прилагаются сведения:

об активах объекта информационной инфраструктуры с указанием сетевых (IP) адресов и названий физических серверов, виртуальных машин, контейнеров, обеспечивающих их функционирование;

о средствах защиты информации с указанием сетевых (IP) адресов их администрирования;

об открытых портах транспортного уровня с указанием соответствующих им протоколов и сетевых (IP) адресов активов объекта информационной инфраструктуры, средств защиты информации;

об используемых доменных именах и сетевых (IP) адресах, посредством которых осуществляется внешнее информационное взаимодействие.

В структурной и логической схемах объекта информационной инфраструктуры допускается объединение однотипных физических устройств, виртуальных машин, относящихся к активам объекта информационной инфраструктуры, средствам защиты информации, в единый элемент при условии наличия соответствующих обозначений, раскрывающих состав данного элемента.

Структурная и логическая схемы объекта информационной инфраструктуры, а также прилагаемые к ним документы составляются в произвольной форме с учетом особенностей функционирования объекта информационной инфраструктуры, а в случае их хранения на бумажных носителях должны быть напечатаны четким шрифтом и поддаваться восприятию (прочтению).

14. В плане должны быть определены:

события (условия), при возникновении которых проводятся мероприятия, предусмотренные планом;

персональный состав команды реагирования, ее задачи и функции;

состав лиц (помимо команды реагирования), привлекаемых для проведения мероприятий по реагированию на киберинциденты;

наименование объекта информационной инфраструктуры;

перечни:

мероприятий по реагированию на киберинциденты, включая сроки их проведения и последовательность действий, совершаемых командой реагирования, исходя из особенностей функционирования объекта информационной инфраструктуры;

средств, необходимых для проведения мероприятий по реагированию на киберинциденты;

мероприятий по восстановлению функционирования объекта информационной инфраструктуры.

15. Договор на оказание услуг по обеспечению кибербезопасности помимо существенных условий, установленных законодательством, должен содержать:

15.1. сведения об объектах информационной инфраструктуры;

15.2. обязательства государственного органа и иной организации, создавших центр кибербезопасности, по:

выявлению киберинцидентов, реагированию на киберинциденты и ликвидации их последствий (в том числе удаленно) с установлением причин возникновения киберинцидентов;

выявлению критических уязвимостей;

уведомлению Национального центра кибербезопасности о выявлении киберинцидентов высокого и среднего уровней, а также критических уязвимостей не позднее одного часа с момента выявления этих киберинцидентов и уязвимостей;

проведению аудита кибербезопасности и оценки эффективности защищенности;

разработке в сроки, установленные в договоре, регламентов и планов;

15.3. обязательства государственного органа и иной организации, которым оказываются услуги по обеспечению кибербезопасности, по:

выполнению в сроки, установленные в договоре, требований по кибербезопасности, если такие требования не выполнены или выполнены не в полном объеме;

предоставлению центру кибербезопасности в сроки, установленные в договоре, сведений, необходимых для выполнения обязательств государственного органа и иной организации, создавших центр кибербезопасности;

15.4. обязательства сторон по выполнению регламентов и планов.

16. Копия договора на оказание услуг по обеспечению кибербезопасности направляется государственными органами и иными организациями, которыми приобретены эти услуги, в ОАЦ в течение пяти рабочих дней со дня его заключения.

В случае расторжения договора на оказание услуг по обеспечению кибербезопасности государственные органы и иные организации, центры кибербезопасности которых оказывали эти услуги, уведомляют об этом ОАЦ в течение пяти рабочих дней со дня расторжения договора.

Приложение 3
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ТИПОВАЯ СТРУКТУРА
ЦЕНТРОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ИНЫХ ОРГАНИЗАЦИЙ

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. Руководитель центра обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственного органа и иной организации (далее - центр кибербезопасности).

2. Заместитель руководителя центра кибербезопасности <*>.

3. Лицо (лица), ответственное (ответственные) за проведение аудита кибербезопасности.

4. Лица, ответственные за выявление киберинцидентов.

5. Лица, ответственные за сбор и обработку событий кибербезопасности.

6. Лица, ответственные за администрирование активов объекта информационной инфраструктуры, эксплуатируемого центром кибербезопасности, и применяемых на этом объекте средств защиты информации.

7. Лицо (лица), ответственное (ответственные) за проведение анализа вредоносного программного обеспечения <**>.

8. Лицо (лица), ответственное (ответственные) за проведение оценки эффективности защищенности объектов информационной инфраструктуры от кибератак <**>.

<*> По решению государственного органа и иной организации может вводиться должность заместителя руководителя центра кибербезопасности.

<**> Должности лиц, ответственных за проведение анализа вредоносного программного обеспечения и оценки эффективности защищенности объектов информационной инфраструктуры от кибератак, могут отсутствовать в структуре центров кибербезопасности, не оказывающих услуги по обеспечению кибербезопасности другим государственным органам и иным организациям. В таком случае для проведения анализа вредоносного программного обеспечения и оценки эффективности защищенности объектов информационной инфраструктуры от кибератак вместо указанных лиц на основании гражданско-правовых договоров могут привлекаться юридические лица, созданные в соответствии с законодательством Республики Беларусь, с местонахождением в Республике Беларусь, а также индивидуальные предприниматели, зарегистрированные в Республике Беларусь.

Приложение 4
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ТРЕБОВАНИЯ
ПО КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ИНЫХ ОРГАНИЗАЦИЙ

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. В отношении объектов информационной инфраструктуры государственных органов и иных организаций должны обеспечиваться следующие требования по кибербезопасности:

для каждого объекта информационной инфраструктуры, границы которого определяются собственником (владельцем) такого объекта, должны быть разработаны и поддерживаться в актуальном состоянии его структурная и логическая схемы;

установленные по умолчанию идентификационные и аутентификационные сведения (реквизиты доступа) к активам объекта информационной инфраструктуры и средствам защиты информации должны быть изменены либо заблокированы возможности их использования (за исключением случаев, когда такие возможности ограничены производителем). Пароли, используемые в качестве аутентификационных сведений, подлежат регулярному обновлению и должны храниться в условиях, исключающих свободный доступ к ним;

доступ к активам объекта информационной инфраструктуры и средствам защиты информации должен осуществляться при условии успешной идентификации и аутентификации пользователей (за исключением случаев, когда такие возможности ограничены производителем) с применением механизмов регистрации, блокировки (при превышении количества неудачных попыток входа) и своевременным удалением или деактивацией неиспользуемых учетных записей по истечении допустимого срока бездействия;

управление доступом к активам объекта информационной инфраструктуры и средствам защиты информации должно осуществляться с использованием модели разграничения доступа, реализующей принцип минимально необходимых привилегий, с обязательной регистрацией и контролем событий по изменению прав доступа и регулярной верификацией актуальности назначенных прав;

доступ к функциям администрирования активов объекта информационной инфраструктуры и средств защиты информации должен быть ограничен и осуществляться только с обязательной регистрацией всех попыток доступа;

программное обеспечение, относящееся к активам объекта информационной инфраструктуры и применяемым на этом объекте средствам защиты информации, должно обновляться до актуальных версий в течение месяца с даты выхода обновления (за исключением случаев, когда возможность такого обновления ограничена производителем, а также случаев, влекущих нарушение или прекращение функционирования таких активов и средств);

системное время для активов объекта информационной инфраструктуры и применяемых на этом объекте средств защиты информации должно быть синхронизировано от единого источника времени;

внешнее информационное взаимодействие должно осуществляться с применением

межсетевого экранирования, обеспечивающего фильтрацию трафика по протоколам сетевого и транспортного уровней, а также контролироваться средствами обнаружения и предотвращения вторжений;

должны быть организованы сбор и обработка сведений о событиях кибербезопасности, а также хранение этих сведений в течение не менее одного года;

активы объекта информационной инфраструктуры должны быть защищены от вредоносного программного обеспечения.

2. Способы реализации требований, указанных в пункте 1 настоящего приложения, определяются государственными органами и иными организациями самостоятельно с учетом особенностей функционирования принадлежащих им объектов информационной инфраструктуры.

3. Работы по реализации требований, указанных в пункте 1 настоящего приложения, в государственном органе и иной организации проводятся подразделением защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации.

В случае невозможности выполнения соответствующих работ силами подразделения защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации, могут привлекаться юридические лица, созданные в соответствии с законодательством Республики Беларусь, с местонахождением в Республике Беларусь, а также индивидуальные предприниматели, зарегистрированные в Республике Беларусь.

Приложение 5
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ПЕРЕЧЕНЬ
ТЕРМИНОВ И ИХ ОПРЕДЕЛЕНИЙ

(введен приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. Автоматизированная система информационного взаимодействия - программное обеспечение, относящееся к активам объекта информационной инфраструктуры, эксплуатируемого Национальным центром обеспечения кибербезопасности и реагирования на киберинциденты, предназначенное для регистрации киберинцидентов, направления и получения уведомлений (запросов) и иной информации в рамках информационного взаимодействия элементов национальной системы обеспечения кибербезопасности, а также для других целей, связанных с обеспечением кибербезопасности.

2. Активы объекта информационной инфраструктуры - средства вычислительной техники, телекоммуникационное оборудование, системное и прикладное программное обеспечение, входящие в состав объекта информационной инфраструктуры и обеспечивающие его функционирование.

3. Аудит кибербезопасности - документированный процесс получения информации о

деятельности государственных органов и иных организаций по обеспечению кибербезопасности принадлежащих им объектов информационной инфраструктуры и установлению степени соответствия выполнения требований, установленных законодательством, регулирующим отношения в области обеспечения кибербезопасности и защиты информации.

4. Индикаторы компрометации - сведения технического характера, которые фактически или потенциально могут свидетельствовать о возникновении киберинцидента.

5. Критическая уязвимость - особенность функционирования программного обеспечения или ошибка программного кода, с использованием которых у неаутентифицированного и (или) непривилегированного пользователя имеется реальная возможность нарушить конфиденциальность, целостность, подлинность, доступность или сохранность информации, обрабатываемой объектом информационной инфраструктуры.

6. Недопустимое событие кибербезопасности - действия или бездействие пользователей активов объектов информационной инфраструктуры, средств защиты информации либо состояние таких активов и средств, которые могут свидетельствовать о возникновении киберинцидента.

7. Оценка эффективности защищенности объектов информационной инфраструктуры от кибератак - комплекс мероприятий, проводимый в государственных органах и иных организациях для выявления уязвимостей, а также иных факторов, которые могут быть использованы для проведения кибератак.

8. Системы классификации уязвимостей - существующие международные или принятые в отдельных государствах перечни (реестры, базы данных) известных уязвимостей в активах объектов информационной инфраструктуры.

9. Система обработки сведений о киберинцидентах - программное обеспечение, относящееся к активам объектов информационной инфраструктуры, эксплуатируемых центрами обеспечения кибербезопасности и реагирования на киберинциденты государственных органов и иных организаций, предназначенное для сбора, обработки и хранения недопустимых событий кибербезопасности, регистрации киберинцидентов, направления и получения уведомлений (запросов) и иной информации в рамках информационного взаимодействия этих центров с государственными органами и иными организациями, а также для других целей, связанных с обеспечением кибербезопасности.

10. Событие кибербезопасности - действия или бездействие пользователей активов объектов информационной инфраструктуры, средств защиты информации либо состояние таких активов и средств, которые могут иметь отношение к кибербезопасности.

11. Уязвимость - особенность функционирования программного обеспечения или ошибка программного кода, с использованием которых у неаутентифицированного и (или) непривилегированного пользователя имеется потенциальная возможность нарушить конфиденциальность, целостность, подлинность, доступность или сохранность информации, обрабатываемой объектом информационной инфраструктуры.

УТВЕРЖДЕНО
Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ЭЛЕМЕНТОВ НАЦИОНАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. В настоящем Положении определяется порядок информационного взаимодействия элементов национальной системы обеспечения кибербезопасности.

2. Информационное взаимодействие государственных органов и иных организаций, создавших центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры (далее - центры кибербезопасности), с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее - ОАЦ) осуществляется посредством системы межведомственного электронного документооборота государственных органов Республики Беларусь и автоматизированной системы государственной защищенной электронной почты ДСП.

Информационное взаимодействие государственных органов и иных организаций, не указанных в части первой настоящего пункта, с ОАЦ осуществляется посредством системы межведомственного электронного документооборота государственных органов Республики Беларусь, автоматизированной системы государственной защищенной электронной почты ДСП и почтовой связи.

3. Информационное взаимодействие центров кибербезопасности с Национальным центром обеспечения кибербезопасности и реагирования на киберинциденты (далее - Национальный центр кибербезопасности) осуществляется посредством автоматизированной системы информационного взаимодействия.

Для организации информационного взаимодействия, указанного в части первой настоящего пункта, центры кибербезопасности:

проводят организационно-технические мероприятия в соответствии с гражданско-правовыми договорами, заключаемыми государственными органами и иными организациями, создавшими эти центры, с обществом с ограниченной ответственностью "Белорусские облачные технологии", за исключением случаев, когда имеются организованные по согласованию с ОАЦ каналы взаимодействия;

представляют в Национальный центр кибербезопасности актуальную схему информационного взаимодействия с Национальным центром кибербезопасности с указанием точек подключения и сетевой (IP) адресации в течение суток с момента ее формирования (обновления).

Информационное взаимодействие с использованием автоматизированной системы информационного взаимодействия осуществляется после принятия решения об аттестации центра кибербезопасности.

Для повышения оперативности информационного взаимодействия центров кибербезопасности с Национальным центром кибербезопасности наряду с автоматизированной системой информационного взаимодействия могут использоваться:

электронная почта, размещенная в национальном сегменте глобальной компьютерной сети Интернет (далее - электронная почта);

телефонная связь;

иные согласованные между ними способы информационного взаимодействия.

4. Информационное взаимодействие государственных органов и иных организаций с Национальным центром кибербезопасности осуществляется посредством электронной почты (в том числе в целях реализации абзаца второго части первой подпункта 3.3 пункта 3 Указа Президента Республики Беларусь от 14 февраля 2023 г. N 40) и телефонной связи.

При невозможности осуществления информационного взаимодействия государственных органов и иных организаций с Национальным центром кибербезопасности в порядке, предусмотренном в части первой настоящего пункта, такое взаимодействие может быть организовано иными способами, не запрещенными законодательством.

5. Информационное взаимодействие государственных органов и иных организаций с центрами кибербезопасности осуществляется:

в порядке, установленном этими органами и организациями, - для взаимодействия с созданными ими центрами кибербезопасности;

в порядке, согласованном между этими органами, организациями и центрами, - при заключении договора на оказание услуг по обеспечению кибербезопасности.

6. Центры кибербезопасности не позднее одного часа с момента выявления киберинцидента высокого или среднего уровня, а также критической уязвимости информируют об этом Национальный центр кибербезопасности и лицо, ответственное 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.

Информация о выявлении киберинцидента высокого или среднего уровня, направляемая в Национальный центр кибербезопасности, должна содержать экземпляр вредоносного программного обеспечения, связанного с возникновением этого киберинцидента (при наличии такого программного обеспечения).

Присвоенный системой обработки сведений о киберинцидентах регистрационный номер является уникальным идентификатором киберинцидента, обязательным для использования при информационном взаимодействии с Национальным центром кибербезопасности.

<*> Государственный орган и иная организация, являющиеся владельцами (собственниками) объектов информационной инфраструктуры, на которых выявлен киберинцидент или критическая уязвимость.

7. Выявленные киберинциденты высокого и среднего уровней регистрируются в автоматизированной системе информационного взаимодействия, и сведения о них хранятся в общереспубликанской базе данных о киберинцидентах (далее - база данных).

В автоматизированной системе информационного взаимодействия могут регистрироваться киберинциденты низкого уровня, а также критические уязвимости.

8. Сведения из базы данных в отношении киберинцидентов, возникших на объектах информационной инфраструктуры государственных органов и иных организаций, могут предоставляться ОАЦ этим государственным органам и организациям по их письменному запросу или запросу в электронной форме. Данные сведения предоставляются в пятнадцатидневный срок со дня поступления запроса. В случае отсутствия в базе данных запрашиваемых сведений государственный орган и иная организация уведомляются об этом в течение пяти рабочих дней со дня поступления запроса.

9. Предоставление государственными органами и иными организациями информации о событиях кибербезопасности и киберинцидентах в иностранные или международные организации осуществляется по согласованию с ОАЦ, если иное не предусмотрено международными договорами Республики Беларусь.

В случае необходимости предоставления информации о событиях кибербезопасности и киберинцидентах в иностранные или международные организации государственные органы и иные организации направляют в ОАЦ письмо с указанием наименования, места нахождения иностранной или международной организации, планируемых к предоставлению сведений и обоснованием необходимости их предоставления.

Согласование предоставления информации или отказ в таком согласовании осуществляется в течение пяти рабочих дней, следующих за днем получения письма, указанного в части второй настоящего пункта, о чем уведомляются государственный орган и иная организация, направившие письмо. В случае отказа в согласовании предоставления информации государственный орган и иная организация уведомляются о причинах отказа.

10. Государственные органы и иные организации, создавшие центры кибербезопасности, до 5 июля (за первое полугодие) и до 5 января (за год) направляют в ОАЦ отчеты о кибербезопасности.

Отчеты о кибербезопасности должны содержать:

сведения о результатах проведенных в отчетном периоде аудитов

кибербезопасности и оценок эффективности защищенности, планах по их проведению в следующем отчетном периоде;

сведения о причинах возникновения киберинцидентов, результатах реагирования на киберинциденты;

сопоставительную таблицу о выполнении каждого из требований к центрам кибербезопасности с указанием формы их реализации;

сведения о государственных органах и иных организациях, которым оказываются услуги по обеспечению кибербезопасности, объектах информационной инфраструктуры, кибербезопасность которых обеспечивается центром кибербезопасности.

Отчеты о кибербезопасности могут содержать предложения по совершенствованию функционирования центров кибербезопасности, а также требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций.

УТВЕРЖДЕНО
Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

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

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. В настоящем Положении определяется порядок 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 и среднего уровней, осуществляет координацию и методическое руководство проведением мероприятий по реагированию на киберинциденты.

Решение об участии национальной команды реагирования в ликвидации последствий киберинцидентов высокого и среднего уровней принимается руководителем Национального центра кибербезопасности по согласованию с начальником Оперативно-аналитического центра при Президенте Республики Беларусь или его уполномоченным заместителем.

3. Реагирование на киберинциденты осуществляется в соответствии с планами мероприятий по реагированию на киберинциденты и с учетом складывающейся обстановки.

Ход реализации мероприятий по реагированию на киберинциденты фиксируется в системе обработки сведений о киберинцидентах.

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

на основании имеющихся индикаторов компрометации определяют перечень объектов информационной инфраструктуры, их активов и применяемых на этих объектах средств защиты информации, вовлеченных в киберинцидент;

осуществляют анализ сведений о событиях кибербезопасности, связанных с киберинцидентами, определяют очередность реагирования на эти события;

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

устанавливают технические параметры киберинцидента;

проводят оценку возможностей (потенциала) внешних и внутренних нарушителей;

осуществляют анализ возможных уязвимостей активов объектов информационной инфраструктуры и применяемых на этих объектах средств защиты информации;

принимают меры по обеспечению сохранности сведений, необходимых для выявления индикаторов компрометации, в соответствии с рекомендациями, размещаемыми на официальном интернет-сайте Оперативно-аналитического центра при Президенте Республики Беларусь;

реализуют иные мероприятия в соответствии с планами мероприятий по реагированию на киберинциденты и складывающейся обстановкой.

5. По результатам реагирования на киберинциденты национальная команда реагирования и команды реагирования выявляют индикаторы компрометации (при их наличии) и формируют отчеты о результатах реагирования на киберинциденты, которые должны содержать:

перечень объектов информационной инфраструктуры, их активов и применяемых на этих объектах средств защиты информации, вовлеченных в киберинцидент;

технические параметры киберинцидента и его последствия;

описание выявленных индикаторов компрометации и причин возникновения киберинцидента;

информацию о восстановлении функционирования объекта информационной инфраструктуры (полное, частичное, восстановление невозможно, восстановление не требуется);

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

описание выявленных нарушений требований по кибербезопасности;

рекомендации по устранению причин возникновения киберинцидента.

Отчеты о результатах реагирования на киберинциденты хранятся в автоматизированной системе информационного взаимодействия.

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

Меры по восстановлению функционирования объектов информационной инфраструктуры и проверке их работоспособности принимаются после завершения мероприятий по устранению киберинцидентов и, как правило, причин их возникновения.

7. При выявлении на объекте информационной инфраструктуры киберинцидентов высокого и среднего уровней до принятия мер по обеспечению сохранности сведений, необходимых для выявления индикаторов компрометации, не допускается:

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

осуществлять поиск и удаление экземпляров вредоносного программного обеспечения;

обновлять программное обеспечение (за исключением выявления наличия на объекте информационной инфраструктуры критических уязвимостей, создающих угрозу возникновения киберинцидентов высокого уровня);

проводить мероприятия по восстановлению информации из резервных копий;

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

8. Центры кибербезопасности на регулярной основе 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.

УТВЕРЖДЕНО
Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
25.07.2023 N 130
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
27.05.2026 N 98)

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ЦЕНТРОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ИНЫХ ОРГАНИЗАЦИЙ

(в ред. приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 27.05.2026 N 98)

1. В настоящем Положении 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 подтверждается соответствие центров кибербезопасности предъявляемым к ним требованиям.

Достаточность теоретических и практических знаний (навыков) работников центров кибербезопасности подтверждается по результатам собеседования и (или) выполнения практических заданий.

Оценка центра кибербезопасности на соответствие предъявляемым требованиям осуществляется в отношении объекта информационной инфраструктуры, эксплуатируемого этим центром.

3. Для проведения аттестации государственные органы и иные организации, создавшие центры кибербезопасности (далее, если не определено иное, - заявитель),

направляют в ОАЦ заявление о проведении аттестации центра кибербезопасности (далее - заявление) в произвольной форме.

К заявлению прилагаются:

сопоставительная таблица о выполнении каждого из предъявляемых к центрам кибербезопасности требований с указанием формы их реализации;

сведения о работниках центра кибербезопасности (фамилия, собственное имя, отчество (если таковое имеется), дата и номер приказа (иного распорядительного документа) о приеме на работу, срок действия трудового договора (контракта), информация об образовании, описание обязанностей, личный номер телефона, адрес электронной почты).

4. Заявление, прилагаемые к нему документы и (или) сведения направляются посредством системы межведомственного электронного документооборота государственных органов Республики Беларусь (далее - СМДО) или автоматизированной системы государственной защищенной электронной почты ДСП.

5. В принятии заявления отказывается в случае нахождения заявителя в процессе ликвидации, представления не всех документов и (или) сведений, указанных в части второй пункта 3 настоящего Положения, а также при отсутствии согласованной с ОАЦ кандидатуры руководителя центра кибербезопасности. Мотивированный отказ в принятии заявления не позднее пяти рабочих дней, следующих за днем поступления заявления в ОАЦ, вместе с заявлением и прилагаемыми к нему документами и (или) сведениями направляется заявителю посредством СМДО или автоматизированной системы государственной защищенной электронной почты ДСП.

6. Решение о проведении аттестации принимается начальником ОАЦ в форме приказа, которым также создается комиссия для проведения аттестации и определяется ее персональный состав.

7. Аттестация может проводиться по месту нахождения заявителя и (или) помещений, которые будут использоваться для осуществления деятельности центра кибербезопасности. В этом случае заявитель посредством СМДО уведомляется о планируемом выезде по месту проведения аттестации, а также о лицах, уполномоченных на проведение аттестации.

Перед началом проведения выездных мероприятий по аттестации уполномоченные на ее проведение лица обязаны предъявить руководителю или иному уполномоченному представителю заявителя служебные удостоверения.

8. По результатам аттестации составляется заключение о соответствии или несоответствии центра кибербезопасности требованиям, предъявляемым к таким центрам. Заключение подписывается лицами, уполномоченными на проведение аттестации, и учитывается при принятии ОАЦ решений об аттестации или об отказе в аттестации центра кибербезопасности.

9. Решение об аттестации или об отказе в аттестации центра кибербезопасности принимается в течение 30 рабочих дней со дня поступления заявления и оформляется приказом ОАЦ. О принятом решении заявитель уведомляется в течение трех рабочих дней со дня его принятия. В случае принятия решения об отказе в аттестации центра кибербезопасности заявитель также уведомляется о выявленных недостатках.

10. Основаниями для принятия решения об отказе в аттестации центра кибербезопасности являются:

указание в заявлении, прилагаемых к нему документах и (или) сведениях недостоверной информации;

наличие в заключении выводов о несоответствии центра кибербезопасности требованиям, предъявляемым к таким центрам.

11. После устранения недостатков, повлекших принятие решения об отказе в аттестации центра кибербезопасности, заявитель вправе вновь обратиться в ОАЦ с заявлением о проведении аттестации, но не ранее чем через два месяца со дня принятия указанного решения.

12. Сведения об аттестованных центрах кибербезопасности размещаются на официальном интернет-сайте ОАЦ.

13. Аттестованные центры кибербезопасности подлежат переаттестации с периодичностью не реже одного раза в три года.

Переаттестация проводится в порядке, установленном для проведения аттестации.

О планируемом проведении переаттестации центра кибербезопасности заявителю направляется уведомление посредством СМДО не позднее чем за три рабочих дня до начала ее проведения.

Решение об аттестации или об отказе в аттестации центра кибербезопасности по результатам переаттестации принимается не позднее 30 рабочих дней со дня направления уведомления, указанного в части третьей настоящего пункта.

14. В случае принятия решения об отказе в аттестации центра кибербезопасности по результатам переаттестации:

14.1. государственный орган и иная организация, создавшие такой центр кибербезопасности:

в течение трех рабочих дней уведомляют о принятии указанного решения другие государственные органы и иные организации, которым оказываются услуги по обеспечению кибербезопасности;

вправе после устранения несоответствий, послуживших основанием для принятия решения об отказе в аттестации этого центра, по истечении срока, указанного в пункте 11 настоящего Положения, вновь обратиться в ОАЦ с заявлением о проведении аттестации;

в течение шести месяцев со дня принятия такого решения заключают договоры о приобретении услуг по обеспечению кибербезопасности у других организаций, создавших центры кибербезопасности (кроме случаев, когда в течение этого срока ОАЦ принято решение об аттестации центра кибербезопасности по заявлению, поданному в соответствии с абзацем третьим настоящего подпункта), если обязанность создания центра кибербезопасности или приобретения услуг по обеспечению кибербезопасности предусмотрена законодательством;

14.2. договоры на оказание этим центром услуг по обеспечению кибербезопасности должны быть расторгнуты и обязательства по ним прекращены в течение шести месяцев со дня принятия указанного решения (кроме случаев, когда в течение этого срока ОАЦ принято решение об аттестации центра кибербезопасности по заявлению, поданному в соответствии с абзацем третьим подпункта 14.1 настоящего пункта).

15. Принятое по результатам проведения аттестации (переаттестации) решение может быть обжаловано заявителем в судебном порядке.
