

ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ
И РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ



РЕКОМЕНДАЦИИ
ГОСУДАРСТВЕННЫМ ОРГАНАМ И ИНЫМ ОРГАНИЗАЦИЯМ
(В ТОМ ЧИСЛЕ ВЛАДЕЛЬЦАМ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ
ИНФОРМАТИЗАЦИИ) ПО ВЫПОЛНЕНИЮ ОБЯЗАТЕЛЬНЫХ ДЛЯ
ИСПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ
ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ
ИНФОРМАЦИИ, ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

При подготовке документа использована
информация, актуальная
на 1 сентября 2024 г.

г.Минск

ОГЛАВЛЕНИЕ

1. ОТВЕТСТВЕННЫЕ ЛИЦА	5
2. ПРЕДЪЯВЛЯЕМЫЕ ТРЕБОВАНИЯ.....	8
2.1. ОИИ, предназначенные исключительно для обработки общедоступной информации и общедоступных персональных данных.....	8
2.2. ИС, предназначенные для обработки ИРиПКО.....	13
2.2.1. Проектирование системы защиты информации.....	18
2.2.2. Создание системы защиты информации	26
2.2.3. Аттестация системы защиты информации	28
2.2.4. Эксплуатация ИС с применением аттестованной в установленном порядке системы защиты информации.....	32
2.2.5. Обеспечение защиты информации в случае прекращения эксплуатации ИС.....	33
2.3. КВОИ	34
2.3.1. Проектирование системы информационной безопасности	41
2.3.2. Создание системы информационной безопасности.....	43
2.3.3. Аудит системы информационной безопасности	47
2.4. Обязательные требования по безопасности использования национального сегмента сети Интернет.....	49
3. МОНИТОРИНГ КИБЕРБЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ	52
3.1. Создание центров кибербезопасности	53
3.2. Приобретение услуг по обеспечению кибербезопасности.....	56
4. ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ С ОАЦ.....	60
4.1. Информационное взаимодействие вне Национальной системы обеспечения кибербезопасности	60
4.2. Информационное взаимодействие в Национальной системе обеспечения кибербезопасности	61
4.3. Особенности информационного взаимодействия с центрами кибербезопасности.....	63
4.4. Обмен информацией с иностранными и международными организациями.....	66
5. ФУНКЦИОНИРОВАНИЕ НАЦИОНАЛЬНОЙ КОМАНДЫ РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ (CERT.BY), КОМАНД	

РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ ЦЕНТРОВ КИБЕРБЕЗОПАСНОСТИ	68
6. ПЕРЕЧЕНЬ ОСНОВНЫХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ	73



АННОТАЦИЯ

С момента создания информационно-коммуникационных технологий (далее – ИКТ) они превратились в основу современного государственного управления, бизнеса и мировой экономики в целом. В настоящее время государства по всему миру не могут игнорировать преимущества, предоставляемые в связи с применением ИКТ.

Вместе с тем повсеместное распространение ИКТ и, как следствие, экспоненциальный рост объема информации, которая уже приобрела статус очередной «нефти», не только способствовали прогрессу, но и появлению новых рисков, вызовов и угроз. В то время как зависимость нашего общества от ИКТ растет, сами технологии остаются изначально уязвимыми. Конфиденциальности, целостности и доступности информации, обрабатываемой с использованием средств автоматизации, угрожают быстро меняющиеся риски киберпространства. При этом преобразующая сила ИКТ как катализаторов экономического роста и социального развития находится в критической точке, когда доверие населения и организаций к использованию таких технологий подрывается отсутствием кибербезопасности.

В этой связи неслучайно, что нарушение киберустойчивости национального сегмента сети Интернет, критически важных объектов информатизации (далее – КВОИ) и государственных информационных систем (далее – ГИС) определяется одной из основных угроз национальной безопасности (абзац двадцать восьмой пункта 29 Концепции национальной безопасности Республики Беларусь, утвержденной решением Всебелорусского народного собрания от 25 апреля 2024 г. № 5).

В целях достижения максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры (далее – ОИИ) Национальным центром кибербезопасности, созданным в структуре Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) подготовлены настоящие рекомендации, направленные на обеспечение безопасного функционирования ОИИ, в том числе КВОИ, с отдельными комментариями по их реализации.

1. ОТВЕТСТВЕННЫЕ ЛИЦА

Согласно части четвертой статьи 29 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон № 455) государственные органы и юридические лица, осуществляющие обработку информации, распространение и (или) предоставление которой ограничено (далее – ИРиПКО), определяют соответствующие подразделения или должностных лиц, ответственных за обеспечение защиты информации (одна из мер по защите информации). При этом в соответствии с частью пятой статьи 28 Закона № 455 не допускается эксплуатация ГИС без реализации мер по защите информации, т.е. во всех государственных органах и организациях в обязательном порядке должны быть определены такие подразделения или должностные лица.

В то же время, персональная ответственность за организацию работ по технической и криптографической защите информации (далее – ТКЗИ) в организации, обеспечение кибербезопасности организации возложена на ее руководителя (пункт 15 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (далее – Указ № 196), обеспечение кибербезопасности организации (подпункт 3.15 пункта 3 Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (далее – Указ № 40)).

Так, например, согласно пункту 5 Декрета Президента Республики Беларусь от 26 июля 1999 г. № 29 «О дополнительных мерах по совершенствованию трудовых отношений, укреплению трудовой и исполнительской дисциплины» неисполнение Конституции Республики Беларусь, решений Президента Республики Беларусь, законов Республики Беларусь, постановлений Совета Министров Республики Беларусь и судебных постановлений при осуществлении должностных обязанностей следует считать грубым нарушением трудовых обязанностей, что, в свою очередь, позволяет прекратить трудовой договор с руководителем до истечения срока его действия (пункт 1 части первой статьи 47 Трудового кодекса Республики Беларусь).

В соответствии с абзацем четвертым подпункта 4.2 пункта 4 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций» противоправные действия (бездействие) руководителя организации, установленные законодательными актами, признаются грубым нарушением трудовых обязанностей, влекущим безусловное

привлечение руководителя организации к дисциплинарной ответственности вплоть до увольнения с занимаемой должности.

Непринятие руководителем юридического лица или иным лицом, занимающим руководящую должность, необходимых мер по надлежащей организации деятельности этого юридического лица в соответствии с установленными законодательством требованиями, повлекшее причинение вреда государственным или общественным интересам, окружающей среде, жизни, здоровью, правам и законным интересам граждан, если в этом деянии нет состава иного административного правонарушения, влечет наложение штрафа в размере от десяти до двухсот базовых величин согласно статье 24.58 Кодекса Республики Беларусь об административных правонарушениях.

Статьей 203-2 Уголовного кодекса Республики Беларусь (далее – УК) установлена ответственность за несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий. При этом согласно абзацу шестому пункта 3 статьи 17 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» одной из обязательных мер по обеспечению защиты персональных данных является их техническая и криптографическая защита.

За исключением указанного, УК не содержит специальных составов, предусматривающих ответственность за нарушения законодательства в сферах обеспечения кибербезопасности, ТКЗИ. В этой связи к группе уголовно наказуемых противоправных деяний, выражающихся в формировании причин и условий, способствующих совершению преступлений, объектом посягательств которых выступают общественные отношения, связанные с безопасным функционированием трех упомянутых групп ОИИ, относятся преступления против интересов службы (глава 35 УК): бездействие должностного лица (статья 425 УК), служебная халатность (статья 428 УК) и др., совершенные должностным лицом (руководителем) организации, на которого возложена персональная ответственность за организацию работ по ТКЗИ, а также обеспечение кибербезопасности возглавляемой организации.

Ответственность руководителя обусловлена его ролью в принятии управленческих решений, связанных, прежде всего, с финансированием работ по обеспечению безопасности ОИИ. Нередко высокая стоимость соответствующих работ в совокупности с отсутствием понимания возможных негативных последствий кибератак и вызванных ими киберинцидентов приводит к непринятию (отказу в согласовании) комплекса правовых, организационных и технических мер, направленных на обеспечение защищенности ОИИ и содержащейся в них информации

от внутренних и внешних угроз. В отдельных случаях такие решения могут приниматься руководителями осознанно, исходя из наличия личной заинтересованности (например, финансирование, необходимое для обеспечения кибербезопасности ОИИ, проектирования, создания и аттестации системы защиты информации, проектирования, создания и аудита системы информационной безопасности, может перенаправляться на решение вопросов в целях достижения показателей премирования) и др.



2. ПРЕДЪЯВЛЯЕМЫЕ ТРЕБОВАНИЯ

На 1 сентября 2024 г. в Республике Беларусь выделены три основные группы ОИИ с различными предъявляемыми требованиями по обеспечению их защиты и защиты обрабатываемой в них информации (без учета группы объектов информатизации, предназначенных для обработки государственных секретов).

Также в стране действует ряд обязательных требований по безопасности использования национального сегмента глобальной компьютерной сети Интернет (далее – сеть Интернет).

2.1. ОИИ, предназначенные исключительно для обработки общедоступной информации и общедоступных персональных данных

К первой группе относятся ОИИ, предназначенные исключительно для обработки общедоступной информации и общедоступных персональных данных.

Согласно статье 15 Закона Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации» (далее – Закон № 455-3) в зависимости от категории доступа информация делится на общедоступную информацию и ИРиПКО.

К общедоступной информации (статья 16 Закона № 455-3) относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не может быть ограничен доступ к информации, распространение и (или) предоставление информации:

- о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;

- о деятельности государственных органов, общественных объединений;

- о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами;

- о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;

- о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

- о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

- о состоянии преступности, а также о фактах нарушения законности;

о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

о размерах золотого запаса;

об обобщенных показателях по внешней задолженности;

о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

накапливаемой в открытых фондах библиотек и архивов, информационных системах (далее – ИС) государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

В свою очередь, к общедоступным персональным данным относятся персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов (статья 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон № 99-З). Выделение общедоступных персональных данных обусловлено возможностью фактически любого лица получить доступ к таким данным. В этой связи Законом № 99-З установлен «облегченный» правовой режим обработки таких данных.

При этом под распространением персональных данных понимаются действия, направленные на ознакомление с персональными данными неопределенного круга лиц, что отличает их от предоставления персональных данных, то есть действий, направленных на ознакомление с персональными данными определенного лица или круга лиц.

Обязательные к реализации требования по кибербезопасности таких объектов определены приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (далее – приказ ОАЦ № 130) (приложение 4). К ним относятся:

1. Использование технических, программно-аппаратных и программных средств, в том числе средств защиты информации, размещенных на территории Республики Беларусь.

Справочно. При этом речь идет о технических, программно-аппаратных и программных средствах, в том числе о средствах защиты информации, используемых для обеспечения кибербезопасности.

2. Применение средств защиты информации, прошедших подтверждение соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ) (далее – ТР 2013/027/ВУ), утвержденного постановлением Совета

Министров Республики Беларусь от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ)» (далее – постановление № 375).

Справочно. При этом допускается подтверждение соответствия средств защиты информации как путем сертификации, так и путем декларирования соответствия.

3. Наличие структурной и логической схем ОИИ, поддержание таких схем в актуальном состоянии.

Справочно. Структурная схема должна содержать расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированных рабочих мест администратора (оператора).

В логической схеме должны быть отображены ОИИ, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств.

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

Справочно. В рамках реализации данного требования необходимо регламентировать соответствующий порядок:

определить требования к паролям, частоте их смены, в том числе для различных групп пользователей (при необходимости);

установить правила обновления программного обеспечения, в том числе к средствам защиты информации (такие правила должны минимизировать влияние на рабочие процессы организации).

Конкретные требования законодательством не предъявляются, то есть собственник (владелец) ОИИ, учитывая понимание особенностей своей деятельности, возможных внешних и внутренних угроз, должен самостоятельно определять набор соответствующих требований в локальных правовых актах, обязательных к исполнению в организации. При этом реализация установленного порядка может осуществляться как с применением технических, так и организационных мер.

5. Изменение установленных по умолчанию идентификационных и аутентификационных данных (реквизитов доступа) к ОИИ, в том числе к средствам защиты информации, либо блокирование возможности их использования.

Справочно. В рамках реализации данного требования необходимо изменить соответствующие реквизиты доступа, установленные

по умолчанию, там, где это возможно. В последующем – осуществлять их смену в соответствии с регламентом, разработанным в рамках пункта 4 настоящих требований.

6. Использование модели управления доступом (разграничения доступа) к ОИИ, в том числе к средствам защиты информации.

Справочно. При реализации данного требования следует руководствоваться принципом назначения минимальных привилегий, то есть пользователь должен иметь доступ только к тем ОИИ, в том числе к средствам защиты информации, и только в том объеме, которые абсолютно необходимы для решения стоящих перед ним задач. Повышение привилегий «на всякий случай» должно быть исключено.

7. Идентификация и аутентификация пользователей, своевременное блокирование (удаление) неиспользуемых идентификационных данных пользователей.

Справочно. Каждый пользователь ОИИ должен быть строго определен. Использование «общих» учетных записей не должно допускаться. Неиспользуемые идентификационные данные пользователей (например, используемые лицами, с которыми трудовые отношения прекращены) должны своевременно блокироваться (удаляться).

8. Регламентированный доступ к настройкам (администрированию) ОИИ, в том числе средств защиты информации.

Справочно. Доступ к настройкам (администрированию) ОИИ, в том числе к средствам защиты информации, должен быть зафиксирован в регламенте и обеспечиваться в строгом соответствии с правилами, описанными в таком регламенте.

9. Синхронизация системного времени от единого (общего) источника.

Справочно. Время на всех устройствах должно быть синхронизировано с общим NTP-устройством. Выбор такого устройства определяется собственником (владельцем) ОИИ.

10. Межсетевое экранирование при внешнем информационном взаимодействии по портам протоколов сетевого и транспортного уровней.

Справочно. Внешнее информационное взаимодействие в обязательном порядке должно быть ограничено по IP-адресам и портам транспортного уровня. При этом лучшей практикой является использование последнего правила в листе доступа межсетевого экрана: «Запретить все остальное».

11. Обнаружение и предотвращение вторжений при внешнем информационном взаимодействии.

Справочно. Внешнее информационное взаимодействие должно осуществляться при условии применения решений типа IDS (данные системы анализируют трафик и активность приложений для выявления подозрительных действий, которые могут указывать на попытку

вторжения) / IPS (активно блокируют обнаруженные атаки, предотвращая их распространение и минимизируя риск человеческой ошибки).

12. Защита от воздействия вредоносных программ.

Справочно. Такая защита реализуется посредством применения антивирусных решений (хостовых или потоковых).

Хостовые антивирусы обеспечивают защиту на уровне отдельных устройств или серверов. Сканируют файлы и приложения на наличие вредоносного кода, используя базы данных сигнатур вирусов и поведенческий анализ для обнаружения подозрительной активности.

Потоковые антивирусы работают на уровне сети, анализируя трафик данных, проходящий через сетевые устройства, такие как маршрутизаторы и шлюзы. Предназначены для обнаружения и блокирования вредоносных программ до того, как они достигнут конечных пользователей.

При этом лучшей практикой является использование хостовых антивирусов для каждого хоста.

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

Справочно. Порядок реализации данного требования определяется самостоятельно собственником (владельцем) ОИИ. При этом такой сбор может осуществляться вручную или с использованием средств автоматизации (предпочтительнее).

Перечень типов и записей событий информационной безопасности определен в приложении к Положению о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности, утвержденному приказом ОАЦ № 130 (далее – перечень). Определены для операционных систем, систем управления базами данных, телекоммуникационного оборудования, прикладного программного обеспечения и средств защиты информации.

Государственный орган и иная организация вправе заключить гражданско-правовой договор на выполнение работ (оказание услуг), предусмотренных пунктами 10, 11 и 13 перечня, с поставщиками интернет-услуг и (или) организацией, оказывающими услуги по обеспечению кибербезопасности ОИИ.

Государственным органам и организациям также следует учитывать, что согласно части первой статьи 34 Конституции Республики Беларусь гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, о политической, экономической, культурной и международной жизни, состоянии окружающей среды.

При этом подпунктом 1.1 пункта 1 Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» (далее – Указ № 60) определено, что государственные органы и организации обязаны размещать информацию о своей деятельности на официальных интернет-сайтах в сети Интернет.

В этой связи, например, киберинцидент на ОИИ, обеспечивающем функционирование такого официального интернет-сайта какого-либо государственного органа или организации, вызванный успешно проведенной кибератакой типа «отказ в обслуживании» (DoS/DDoS), следует рассматривать как факт нарушения упомянутых выше конституционных прав граждан, что, в свою очередь, может рассматриваться в качестве «вреда государственным или общественным интересам, правам и законным интересам граждан», входящего в диспозицию состава административного правонарушения, предусмотренного статьей 24.58 КоАП. В отдельных случаях нарушение указанных конституционных прав может признаваться «существенным вредом» (например, согласно части второй пункта 20 постановления Пленума Верховного Суда Республики Беларусь от 16 декабря 2004 г. № 12 «О судебной практике по делам о преступлениях против интересов службы» (статьи 424 – 428 Уголовного кодекса Республики Беларусь (далее – УК).

2.2. ИС, предназначенные для обработки ИРиПКО

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения) и блокирования правомерного доступа к ней.

Ситуация с защитой ИРиПКО иная, поскольку даже неправомерный (несанкционированный) доступ к такой информации значительным образом нарушает права различных субъектов, которые рассчитывают на сохранение конфиденциальности данной информации. Изложенное обязывает государство и должностных лиц реагировать соответствующим образом.

Таким образом, ко второй группе ОИИ относятся ИС, предназначенные для обработки ИРиПКО.

Согласно статье 17 Закона № 455-З к ИРиПКО относится:

информация о частной жизни физического лица и персональные данные (учитывая необходимость обеспечения защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных, в стране принят Закон № 99-З);

сведения, составляющие государственные секреты (правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь определены Законом Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах»);

служебная информация ограниченного распространения (порядок проставления на документах ограничительного грифа «Для служебного пользования» и ведения делопроизводства в государственных органах и государственных организациях, иных юридических лицах, организациях, не являющихся юридическими лицами, по документам, содержащим служебную информацию ограниченного распространения, определен положением, утвержденным постановлением Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну» (далее – постановление № 783);

информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну (в Республике Беларусь принят (издан) целый ряд нормативных правовых актов, определяющих правовой режим различных охраняемых законом тайн: Банковский кодекс Республики Беларусь (статья 121 «Банковская тайна»); Закон «О здравоохранении» (статья 46 «Предоставление информации о состоянии здоровья пациента. Врачебная тайна») и т.д.);

информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу (например, УПК включает статью 198 «Недопустимость разглашения данных предварительного расследования», а Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях – статью 11.5 «Недопустимость разглашения сведений, содержащихся в деле об административном правонарушении»);

иная информация, доступ к которой ограничен законодательными актами (согласно статье 2 Закона Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах» к законодательным актам относятся Конституция Республики Беларусь, законы, декреты и указы Президента Республики Беларусь).

В соответствии с частью четвертой статьи 28 Закона № 455-З ИРиПКО, не отнесенная к государственным секретам, должна обрабатываться в ИС с применением системы защиты информации, аттестованной в порядке, установленном ОАЦ.

Согласно терминологическому аппарату в соответствии с Положением о технической и криптографической защите информации, утвержденным Указом № 196 (далее – Положение о ТКЗИ), под системой защиты информации понимается совокупность мер по защите информации, реализованных в ИС.

При этом пунктом 3 Положения о ТКЗИ названное положение Закона уточняется. В частности, определяется, что требования Положения о ТКЗИ не распространяются на организации, не являющиеся государственными, которые являются собственниками (владельцами) ИС, предназначенных для обработки ИРиПКО, за исключением служебной информации ограниченного распространения, информации о частной жизни физического лица и персональных данных.

Пунктом 3 Положения о ТКЗИ также предусмотрено, что его положения обязательны для применения собственниками (владельцами) ИС, в которых обрабатываются электронные документы, а также организациями, оказывающими услуги по распространению открытых ключей проверки электронной цифровой подписи, аккредитованными в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Таким образом, организации, не являющиеся государственными, из числа собственников (владельцев) ИС, предназначенных для обработки, например, информации, составляющей коммерческую, профессиональную, банковскую и иную охраняемую законом тайну (когда такая информация не относится к служебной информации ограниченного распространения, информации о частной жизни физического лица и персональным данным), вправе обрабатывать такую информацию в ИС без применения аттестованной в установленном порядке системы защиты информации.

Также пунктом 13 Положения о ТКЗИ предусмотрено, что при осуществлении технической и криптографической защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

Как ранее отмечено в структурном элементе 2 настоящих рекомендаций, ТР 2013/027/ВУ, распространяемый на выпускаемые (с 1 января 2014 г.) в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, утвержден постановлением № 375.

Порядок ТКЗИ в ИС, предназначенных для обработки ИРиПКО, определяется одноименным положением (далее – Положение о порядке ТКЗИ в ИС), утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – приказ ОАЦ № 66).

В соответствии с пунктом 3 Положения о порядке ТКЗИ в ИС комплекс мероприятий по ТКЗИ, подлежащей обработке (сбор, накопление, ввод, вывод, прием, передача, запись, хранение, регистрация, уничтожение, преобразование, отображение) в ИС, включает:

- проектирование системы защиты информации;

- создание системы защиты информации;

- аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, за исключением государственных секретов, утвержденным приказом ОАЦ № 66;

- обеспечение функционирования системы защиты информации в процессе эксплуатации ИС;

- обеспечение защиты информации в случае прекращения эксплуатации ИС.

Работы по ТКЗИ у собственника (владельца) ИС могут выполняться:

- подразделением защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации. Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам ТКЗИ в порядке, установленном законодательством;

- организациями, имеющими лицензии на осуществление деятельности по ТКЗИ в части соответствующих составляющих данный вид деятельности работ и (или) услуг (далее – специализированные организации).

До проведения работ по проектированию системы защиты информации собственник (владелец) ИС осуществляет категорирование информации, которая будет обрабатываться в ИС, в соответствии с законодательством об информации, информатизации и защите информации, а также отнесение ИС к классу типовых ИС.

При категорировании информации следует учитывать, что согласно статьям 15 – 18 Закона № 455-З информация делится на общедоступную информацию и ИРиПКО в зависимости от категории доступа.

При этом к общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены, а к ИРиПКО:

информация о частной жизни физического лица и персональные данные;

сведения, составляющие государственные секреты;

служебная информация ограниченного распространения;

информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

иная информация, доступ к которой ограничен законодательными актами.

В соответствии с приложением 1 к Положению о порядке ТКЗИ в ИС определены следующие классы типовых ИС:

1. Класс 6-частн – негосударственные ИС, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

2. Класс 6-гос – государственные ИС, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

3. Класс 5-частн – негосударственные ИС, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

4. Класс 5-гос – государственные ИС, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

5. Класс 4-ин – ИС, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

6. Класс 4-спец – ИС, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

7. Класс 4-бг – ИС, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных.

8. Класс 4-юл – ИС, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну

юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые не имеют подключений к открытым каналам передачи данных.

9. Класс 4-дсп – ИС, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных.

10. Класс 3-ин – ИС, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

11. Класс 3-спец – ИС, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

12. Класс 3-бг – ИС, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.

13. Класс 3-юл – ИС, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных.

14. Класс 3-дсп – ИС, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных.

Отнесение ИС к классу типовых ИС оформляется актом по форме согласно приложению 2 к Положению о порядке ТКЗИ в ИС.

2.2.1. Проектирование системы защиты информации

На этапе проектирования системы защиты информации осуществляются:

анализ структуры ИС и информационных потоков (внутренних и внешних) в целях определения состава (количества) и мест размещения элементов ИС (аппаратных и программных), ее физических и логических границ;

издание политики информационной безопасности;

определение требований к системе защиты информации в техническом задании на создание системы защиты информации (далее – техническое задание);

выбор средств ТКЗИ;

разработка (корректировка) общей схемы системы защиты информации.

Политика информационной безопасности должна содержать:

цели и принципы защиты информации;

перечень ИС, отнесенных к соответствующим классам типовых ИС, перечень средств вычислительной техники, а также сведения о подразделении защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации (если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами);

обязанности пользователей ИС;

порядок взаимодействия с иными ИС (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей ИС и обладателей информации.

Техническое задание разрабатывается собственником (владельцем) ИС либо специализированной организацией и утверждается собственником (владельцем) ИС.

Техническое задание должно содержать:

1. Наименование ИС с указанием присвоенного ей класса типовых ИС.
2. Требования к системе защиты информации в зависимости от используемых технологий и класса типовых ИС на основе перечня согласно приложению 3 к Положению о порядке ТКЗИ в ИС:

Таблица 1

ПЕРЕЧЕНЬ
требований к системе защиты информации
в зависимости от используемых технологий
и класса типовых информационных систем

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
1	Аудит безопасности:										
1.1.	определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники,	+	+	+	+	+	+	+	+	+	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
	сетевого оборудования и средств защиты информации и другое)										
1.2.	обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+
1.3.	обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+/-**	+/-	+	+/-	+/-	+	+	+	+/-	+
1.4.	определение способа и периодичности мониторинга (просмотр, анализ) событий информационной безопасности уполномоченными на это пользователями ИС	+	+	+	+	+	+	+	+	+	+
1.5.	обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+
2.	Требования по обеспечению защиты данных:										
2.1.	регламентация порядка использования в ИС съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+	+	+	+	+
2.2.	обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации	+	+	+	+	+	+	+	+	+	+
2.3.	обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности	+	+	+	+	+	+	+	+	+	+
3.	Требования по обеспечению идентификации и аутентификации:										
3.1.	обеспечение разграничения доступа пользователей	+	+	+	+	+	+	+	+	+	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
	к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации										
3.2.	обеспечение идентификации и аутентификации пользователей ИС	+	+	+	+	+	+	+	+	+	+
3.3.	обеспечение защиты обратной связи при вводе аутентификационной информации	+	+	+	+	+	+	+	+/-	+	+
3.4.	обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей ИС	+	+	+	+	+	+	+	+	+	+
3.5.	обеспечение контроля за соблюдением правил генерации и смены паролей пользователей ИС	+	+	+	+	+	+	+	+	+	+
3.6.	обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей ИС	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+	+
3.7.	обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя ИС или по его запросу	+	+	+	+	+	+	+	+	+	+
4.	Требования по защите системы защиты информации ИС:										
4.1.	обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию	+	+	+	+	+	+	+	+	+	+
4.2.	обеспечение обновления объектов ИС	+	+	+	+	+	+	+	+	+	+
4.3.	обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты ИС	+	+	+	+	+	+	+	+	+	+
4.4.	обеспечение синхронизации временных меток и (или) системного времени в ИС и системе защиты информации	+	+	+	+	+	+	+	+	+	+
5.	Обеспечение криптографической защиты информации:										
5.1.	обеспечение конфиденциальности и контроля целостности	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
	информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации										
5.2.	обеспечение конфиденциальности и контроля целостности информации при ее хранении в ИС (средства предварительного шифрования)	+/-	+/-	+	+/-	+/-	+/-	+/-	+	+/-	+/-
5.3.	обеспечение подлинности и контроля целостности электронных документов в ИС (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)	+	+	+	+	+	+	+	+	+	+
5.4.	обеспечение контроля целостности данных в ИС (средства контроля целостности)	+/-	+/-	+	+/-	+/-	+/-	+/-	+	+/-	+/-
5.5.	обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)	+/-	+/-	+/-	+/-	+	+/-	+/-	+/-	+/-	+
5.6.	обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в ИС (криптографический токен и (или) средства выработки электронной цифровой подписи)	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-
6.	Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре:										
6.1.	обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+
6.2.	обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+
6.3.	обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных	+	+	+	+/-	+/-	+	+	+	+	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
6.4.	обеспечение резервного копирования пользовательских виртуальных машин	+/-	+/-	+	+/-	+	+	+	+	+	+
6.5.	обеспечение резервирования сетевого оборудования по схеме N + 1	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+
6.6.	физическая изоляция сегмента виртуальной инфраструктуры (система хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	+/-	+/-	+/-	+/-	+	+/-	+/-	+/-	+/-	+
7.	Иные требования:										
7.1.	определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+	+	+	+	+
7.2.	обеспечение контроля за составом объектов ИС	+	+	+	+	+	+	+	+	+	+
7.3.	автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+	+
7.4.	использование объектов ИС под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов ИС или особенностей объектов ИС)	+	+	+	+	+	+	+	+	+	+
7.5.	определение состава и содержания информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+
7.6.	обеспечение резервирования информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+
7.7.	обеспечение резервирования конфигурационных файлов сетевого оборудования	+/-	+/-	+	+/-	+	+	+	+	+	+
7.8.	обеспечение обновления программного обеспечения объектов ИС и контроля за своевременностью такого обновления	+	+	+	+	+	+	+	+	+	+
7.9.	обеспечение сегментирования (изоляции) сети управления объектами ИС от сети передачи данных	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+	+
7.10.	обеспечение защиты средств вычислительной техники от вредоносных программ	+	+	+	+	+	+	+	+	+	+
7.11.	обеспечение в реальном масштабе времени	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
	автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ										
7.12.	обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.13.	обеспечение управления внешними информационными потоками (маршрутизация) между ИС. Использование маршрутизатора (коммутатора маршрутизирующего)	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.14.	обеспечение ограничений входящего и исходящего трафика (фильтрация) ИС только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.15.	обеспечение ограничений входящего и исходящего трафика (фильтрация) ИС только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.16.	обеспечение обнаружения и предотвращения вторжений в ИС. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.17.	обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и др.). Использование беспроводных систем обнаружения и предотвращения вторжений	+/ -	+/ -	+/ -	+/ -	+/ -	+	+	+	+	+
7.18.	обеспечение обнаружения утечек информации из ИС. Использование системы обнаружения утечек информации из ИС	+/ -	+/ -	+/ -	+/ -	+/ -	+/ -	+/ -	+/ -	+/ -	+

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем (далее – ИС)									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
7.19.	определение перечня внешних подключений к ИС и порядка такого подключения	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.20.	обеспечение контроля за внешними подключениями к ИС	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.21.	ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+/–	+

*Требования, отмеченные знаком «+», являются обязательными.

**Требования, отмеченные знаком «+/–», являются рекомендуемыми.

В представленной таблице обозначения «4-ин», «4-спец», «4-бг», «4-юл», «4-дсп», «3-ин», «3-спец», «3-бг», «3-юл» и «3-дсп» соответствуют классам типовых ИС.

Требования для ИС, отнесенных к иным классам типовых ИС, приказом ОАЦ № 66 не предъявляются. В то же время собственником (владельцем) данных ИС должны быть реализованы требования по кибербезопасности, описанные в подпункте 2.1 пункта 2 настоящих рекомендаций.

3. Сведения об организации взаимодействия с иными ИС (в случае предполагаемого взаимодействия) с учетом требований согласно приложению 4 к Положению о порядке ТКЗИ в ИС.

4. Порядок обезличивания персональных данных (в случае их обработки в ИС) с применением методов согласно приложению 5 к Положению о порядке ТКЗИ в ИС.

5. Требования из числа реализованных в аттестованной в установленном порядке системе защиты информации ИС другого собственника (владельца) в случае, если функционирование ИС, для которой осуществляется проектирование системы защиты информации, предполагается на базе ИС другого собственника (владельца) в соответствии с пунктом 14 настоящего Положения.

6. Требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита),

криптографическим протоколам, управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются ОАЦ.

7. Перечень документации на систему защиты информации.

Справочно. *Собственник (владелец) ИС вправе не включать в техническое задание отдельные обязательные требования к системе защиты информации при отсутствии в ИС соответствующего объекта (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.*

Общая схема системы защиты информации должна содержать:

наименование ИС;

класс типовых ИС;

места размещения средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств ТКЗИ (далее – объекты ИС);

физические границы ИС;

внешние и внутренние информационные потоки, и протоколы обмена защищаемой информацией.

Допускается создание единой системы защиты информации для:

нескольких ИС, функционирующих в общей программно-технической среде и принадлежащих одному собственнику (владельцу);

нескольких типовых ИС, принадлежащих одному собственнику (владельцу).

При проектировании системы защиты информации ИС, функционирование которой предполагается на базе ИС другого собственника (владельца), имеющей аттестованную систему защиты информации, возможно применение требований, реализованных в системе защиты информации ИС данного собственника (владельца). Такие требования применяются согласно договору на оказание соответствующих услуг.

2.2.2. Создание системы защиты информации

На этапе создания системы защиты информации осуществляются:

внедрение средств ТКЗИ, проверка их работоспособности и совместимости с иными объектами ИС;

разработка (корректировка) документации на систему защиты информации по перечню, определенному в техническом задании;

реализация организационных мер по защите информации.

В ходе внедрения средств ТКЗИ осуществляются:

их монтаж и наладка в соответствии с документацией на систему защиты информации, рекомендациями изготовителя, требованиями по совместимости средств криптографической защиты информации и ограничениями, указанными в сертификате соответствия;

смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов;

проверка корректности выполнения такими средствами требований безопасности в реальных условиях эксплуатации и во взаимодействии с иными объектами ИС.

Документация на систему защиты информации должна содержать описание способов разграничения доступа пользователей к объектам ИС, а также порядок:

- резервирования и уничтожения информации;
- защиты от вредоносного программного обеспечения (далее – ВПО);
- использования съемных носителей информации;
- использования электронной почты;
- обновления средств защиты информации;
- осуществления контроля (мониторинга) за функционированием ИС и системы защиты информации;
- реагирования на события информационной безопасности и ликвидацию их последствий;
- управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

Реализация организационных мер по защите информации осуществляется в целях выполнения требований, изложенных в документации на систему защиты информации собственника (владельца) ИС, которые доводятся до сведения пользователей ИС под роспись.

Организационные меры по криптографической защите информации должны включать меры по обеспечению особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к средствам криптографической защиты информации и криптографическим ключам (носителям), а также по разграничению доступа к ним по кругу лиц.

При получении собственником (владельцем) ИС от физического лица его персональных данных, предоставленных этим физическим лицом без использования средств криптографической защиты информации, предоставление в последующем таких данных тем же собственником (владельцем) ИС названному физическому лицу может осуществляться без использования средств криптографической защиты информации.

2.2.3 Аттестация системы защиты информации

Следующим этапом является аттестация системы защиты информации, в ходе которого документально подтверждается соответствие системы защиты информации требованиям законодательства об информации, информатизации и защите информации.

Аттестация проводится организациями, имеющими лицензии на осуществление деятельности по ТКЗИ в части соответствующих составляющих данный вид деятельности работ (далее – специализированные организации).

При проведении аттестации собственником (владельцем) ИС самостоятельно работы по аттестации выполняются аттестационной комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) ИС. Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) ИС, в которых обрабатываются персональные данные, вправе выполнять работы по аттестации единолично.

Аттестация специализированными организациями проводится на основании следующих исходных данных:

- политики информационной безопасности;
- акта отнесения ИС к классу типовых ИС;
- технического задания на создание ИС или системы защиты информации (техническое задание на создание ИС представляется в случае закрепления в нем требований по защите информации);
- общей схемы системы защиты информации;
- документации на систему защиты информации;
- копий сертификатов соответствия либо экспертных заключений на средства защиты информации.

При проведении аттестации специализированной организацией привлекаются представители собственника (владельца) ИС из состава подразделения защиты информации или иного подразделения (должностное лицо), ответственного за обеспечение защиты информации (если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами).

Аттестация проводится в случаях:

- создания системы защиты информации;
- истечения срока действия аттестата соответствия;
- изменения технологии обработки защищаемой информации;
- изменения технических мер, реализованных при создании системы защиты информации.

Аттестация вновь создаваемой системы защиты информации осуществляется до ввода ИС в эксплуатацию.

Наличие аттестата соответствия является обязательным условием для обработки ИРиПКО, не отнесенной к государственным секретам, в течение установленного в нем срока.

Аттестация предусматривает комплексную оценку системы защиты информации в реальных условиях эксплуатации ИС и включает:

- разработку программы и методики аттестации;

- установление соответствия реального состава и структуры объектов ИС общей схеме системы защиты информации;

- проверку правильности отнесения ИС к классу типовых ИС, выбора и применения средств защиты информации;

- анализ разработанной документации на систему защиты информации собственника (владельца) ИС на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации;

- ознакомление с документацией о распределении функций персонала по организации и обеспечению защиты информации;

- проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации;

- внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС;

- оформление технического отчета и протокола испытаний;

- оформление аттестата соответствия.

Технический отчет должен содержать:

- сроки проведения испытаний;

- вывод о соответствии (несоответствии) реального состава и структуры объектов ИС общей схеме системы защиты информации;

- вывод о выполнении (невыполнении) установленных законодательством требований по защите информации;

- отчет о внешней и внутренней проверке отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС.

При этом при аттестации ИС классов «З-ин», «З-спец», «З-бг», «З-юл» и «З-дсп» следующие мероприятия проводятся с использованием средства контроля эффективности защищенности информации:

проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации;

внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно иницированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС.

Допускается выполнение мероприятий по комплексной оценке системы защиты информации в реальных условиях эксплуатации ИС на выделенном наборе сегментов ИС, обеспечивающих полную реализацию технологии обработки защищаемой информации.

Следует иметь в виду, что мероприятия по комплексной оценке системы защиты информации в реальных условиях эксплуатации ИС могут не проводиться при выполнении в совокупности следующих условий:

аттестация системы защиты информации ИС, создаваемой на базе ИС специализированной организации, проводится этой специализированной организацией;

в системе защиты информации ИС специализированной организации, аттестованной в установленном порядке, реализованы требования по защите информации аттестуемой системы защиты информации.

Программа и методика аттестации разрабатываются на основании исходных данных и должны содержать перечень выполняемых работ с указанием ответственных лиц, сроки выполнения этих работ, информацию о методах проверки требований безопасности, реализованных в системе защиты информации, перечень используемой контрольной аппаратуры и тестовых средств.

Программа и методика аттестации разрабатываются:

аттестационной комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) информационной системы, – при проведении аттестации собственником (владельцем) ИС самостоятельно. Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) ИС, в которых обрабатываются персональные данные, вправе разработать программу и методику аттестации единолично;

специализированной организацией – при проведении аттестации такой организацией. В данном случае специализированная организация

согласовывает разработанные программу и методику аттестации с заявителем.

Срок проведения аттестации:

определяется руководителем собственника (владельца) ИС, физическим лицом, в том числе индивидуальным предпринимателем, являющимся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные, – при проведении аттестации собственником (владельцем) ИС самостоятельно;

не может превышать ста восьмидесяти календарных дней – при проведении аттестации специализированной организацией. В случае выявления в процессе проведения аттестации недостатков специализированная организация не позднее чем за тридцать пять календарных дней до истечения срока проведения аттестации направляет заявителю соответствующее уведомление. Заявитель должен устранить недостатки, выявленные указанной организацией, в течение тридцати календарных дней со дня получения уведомления. При невозможности устранения заявителем выявленных недостатков в указанный срок специализированная организация отказывает в выдаче аттестата соответствия. После устранения недостатков заявитель вправе повторно обратиться за проведением аттестации в порядке, установленном настоящим Положением.

При подтверждении соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации оформляется аттестат соответствия (форма прилагается), который подписывается:

руководителем собственника (владельца) ИС, физическим лицом, в том числе индивидуальным предпринимателем, являющимся собственником (владельцем) ИС, в которой обрабатываются персональные данные, – при проведении аттестации собственником (владельцем) ИС самостоятельно;

руководителем специализированной организации – при проведении аттестации специализированной организацией.

Аттестат соответствия оформляется сроком на пять лет.

АТТЕСТАТ СООТВЕТСТВИЯ
системы защиты информации информационной системы
требованиям по защите информации
от _____ 20__ г. № _____

(наименование информационной системы)

Действителен до _____ 20__ г.

Настоящим аттестатом соответствия удостоверяется, что система защиты информации _____
(наименование информационной системы)

класса _____ соответствует требованиям
(класс типовых информационных систем)
по защите информации, предусмотренным законодательством
и _____
(наименование документов)

Аттестация проведена в соответствии с программой, утвержденной
_____ 20__ г., и методикой, утвержденной _____ 20__ г.

Результаты испытаний приведены в протоколе от _____
20__ г., утвержденном _____
(наименование организации, проводившей испытания)

В информационной системе разрешается обработка информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

При эксплуатации информационной системы запрещается:

Аттестат соответствия действителен при обеспечении неизменности технологии обработки защищаемой информации и совокупности технических и организационных мер, реализованных при создании системы защиты информации.

Руководитель организации

(должность с указанием наименования
организации)

(подпись)

(инициалы, фамилия)

2.2.4. Эксплуатация ИС с применением аттестованной в установленном порядке системы защиты информации

В процессе эксплуатации ИС с применением аттестованной в установленном порядке системы защиты информации осуществляются:

контроль за соблюдением требований, установленных в нормативных правовых актах, документации на систему защиты информации собственника (владельца) ИС;

контроль за порядком использования объектов ИС;

мониторинг функционирования системы защиты информации;

выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования ИС;

резервное копирование информации, содержащейся в ИС;

обучение (повышение квалификации) пользователей ИС.

В соответствии с документацией на систему защиты информации собственники (владельцы) ИС выявляют и фиксируют нарушения требований по защите информации, принимают меры по своевременному устранению таких нарушений.

В случае компрометации криптографических ключей средств криптографической защиты информации собственники (владельцы) ИС обязаны незамедлительно прекратить использование данных средств для обработки информации.

В случае невозможности устранения выявленных нарушений в течение пяти рабочих дней с момента их выявления собственники (владельцы) ИС обязаны:

прекратить обработку информации, распространение и (или) предоставление которой ограничено, о чем письменно проинформировать ОАЦ;

осуществить доработку системы защиты информации и провести оценку на предмет необходимости ее повторной аттестации.

Наладочные работы и сервисное обслуживание объектов ИС проводятся с участием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации (если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами).

Модернизация действующих систем защиты информации осуществляется в порядке, установленном для проектирования и создания таких систем.

2.2.5 Обеспечение защиты информации в случае прекращения эксплуатации ИС

В случае прекращения эксплуатации ИС собственник (владелец) ИС в соответствии с документацией на систему защиты информации принимает меры по:

защите информации, которая обрабатывалась в ИС;

резервному копированию информации и криптографических ключей (при необходимости), обеспечению их конфиденциальности и целостности; уничтожению (удалению) данных и криптографических ключей с машинных носителей информации и (или) уничтожению таких носителей информации.

Государственным органам и организациям следует учитывать, что в условиях повсеместного внедрения средств автоматизированной обработки ИРиПКО обрабатывается в абсолютном большинстве размещенных на территории Республики Беларусь организаций. Даже в тех организациях, основные процессы в которых не связаны с обработкой информации, ее автоматизированная обработка может осуществляться в интересах бухгалтерского и иного обеспечения деятельности организации и т.д.

2.3. КВОИ

К третьей группе ОИИ относятся КВОИ. Такие ОИИ обеспечивают управление технологическими процессами промышленных предприятий, объектами энергетики, информационными процессами банковской сферы, транспорта, систем связи и т.д. Нарушение и (или) прекращение функционирования КВОИ могут привести к самым серьезным негативным последствиям для национальных интересов Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах. В этой связи государство предъявляет к процессу обеспечения безопасности таких объектов особые (наиболее строгие) требования.

Перечень основных владельцев КВОИ представлен в приложении 1 к Указу № 40 (27 организаций). В то же время владелец объекта информатизации имеет право самостоятельно инициировать мероприятия по отнесению таких объектов к критически важным в соответствии с критериями, утвержденными Указом № 196, а также показателями, утвержденными приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь».

В соответствии с Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации, утвержденным Указом № 196 (далее – Положение об отнесении ОИ к КВОИ), критериями отнесения объектов информатизации к критически важным являются:

критерий социальной значимости – в отношении объектов информатизации, обеспечивающих жизнедеятельность населения

(жилищно-коммунальное хозяйство, здравоохранение, образование, труд, занятость и социальная защита);

критерий экономической значимости — в отношении объектов информатизации, обеспечивающих функционирование объектов (организаций) основных отраслей экономики и (или) иные важные экономические потребности, в том числе обеспечивающих проведение безналичных (межбанковских) расчетов, осуществляющих процессинг;

критерий экологической значимости — в отношении объектов информатизации, нарушение или прекращение функционирования которых может причинить ущерб окружающей среде;

критерий информационной значимости — в отношении объектов информатизации в области связи и средств массовой информации.

По состоянию на 1 сентября 2024 г. при отнесении объектов информатизации к критически важным используются следующие показатели уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации, не предназначенного для проведения работ с использованием государственных секретов (его составляющих элементов):

Таблица 2

ПОКАЗАТЕЛИ

уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации, не предназначенного для проведения работ с использованием государственных секретов (его составляющих элементов)

Показатель уровня вероятного ущерба	Уровень вероятного ущерба
Политическая сфера	
1. Ущерб репутации Республики Беларусь на международной арене	Приводит к снижению уровня и интенсивности политического диалога и сотрудничества с зарубежными партнерами в двустороннем, региональном либо в глобальном формате и (или) вызывает экономический ущерб, в том числе в виде санкций, удорожания привлекаемых кредитно-финансовых ресурсов, снижения инвестиционной привлекательности страны, затруднений при приобретении или проведении иных операций с лицензионной продукцией и (или) определенными видами товаров
Экономическая сфера	

Показатель уровня вероятного ущерба	Уровень вероятного ущерба
2. Прекращение или нарушение функционирования объекта информатизации (за исключением объектов Национального банка, банков, небанковских кредитно-финансовых организаций, открытых акционерных обществ «Банк развития Республики Беларусь» и «Белорусская валютно-фондовая биржа»), повлекшие экономический ущерб (прямые и косвенные убытки, включая упущенную выгоду, затраты на ликвидацию последствий прекращения или нарушения функционирования объекта информатизации и восстановление его работоспособности, компенсацию материального ущерба)	Размер ущерба составляет более 100 тыс. базовых величин
3. Невозможность осуществления безналичных межбанковских расчетов в белорусских рублях	Нарушается функционирование на период более двух часов системы, в которой в режиме реального времени осуществляются межбанковские расчеты по срочным и несрочным денежным переводам, а также по результатам клиринга в смежных системах
4. Невозможность осуществления процессинга по операциям в белорусских рублях по платежам, принятым при использовании банковских платежных карточек платежной системы «БЕЛКАРТ», процессинговым центром, удельный вес банковских платежных карточек в авторизационной базе которого в общем по платежной системе составляет более 60 процентов	Нарушается функционирование аппаратно-программного комплекса процессингового центра, удельный вес банковских платежных карточек в авторизационной базе которого в общем по платежной системе «БЕЛКАРТ» составляет более 60 процентов, на период более двух часов
5. Прекращение или нарушение функционирования объекта информатизации, непосредственно управляющего оборудованием подстанции (распределительного устройства электростанции) напряжением 220 кВ и более, имеющей три и более линий электропередачи напряжением 220 кВ и более	Прекращается или нарушается функционирование на период более двух часов
6. Прекращение или нарушение функционирования объекта информатизации, непосредственно управляющего на электростанции блоком единичной мощностью 400 МВт и более	Прекращается или нарушается функционирование на период более двух часов
7. Прекращение или нарушение функционирования объекта информатизации, обеспечивающего непосредственное управление энергетическими объектами с уровня центральной диспетчерской службы и выше	Прекращается или нарушается функционирование на период более двух часов
8. Прекращение или нарушение функционирования объекта информатизации, обеспечивающего управление железнодорожным транспортом на более 50 процентах эксплуатационной длины Белорусской железной дороги	Прекращается или нарушается функционирование на период более двух часов
Социальная сфера	
9. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения (водо-, газо-, тепло-, энергоснабжение, водоотведение)	Нарушается обеспечение жизнедеятельности более 50 тыс. человек

Показатель уровня вероятного ущерба	Уровень вероятного ущерба
10. Несанкционированный доступ к информации о частной жизни физического лица и персональным данным	Количество пострадавших – более 500 тыс. человек
Информационная сфера	
11. Отсутствие доступа к государственным печатным средствам массовой информации и государственным сетевым изданиям населения общей численностью	Более 100 тыс. человек
12. Отсутствие доступа к телепрограммам, входящим в обязательный общедоступный пакет телепрограмм, для населения общей численностью	Более 100 тыс. человек
13. Нарушение функционирования сети передачи данных для населения общей численностью	Более 100 тыс. человек
14. Нарушение предоставления операторам электросвязи доступа к глобальной компьютерной сети Интернет	В отношении одного и более операторов электросвязи
15. Нарушение предоставления доступа к точке обмена национальным трафиком (пиринг) в Республике Беларусь	На период более одного часа
16. Нарушение предоставления операторам электросвязи услуги по пропуску международного и (или) межсетевого трафика	В отношении одного и более операторов электросвязи
Экологическая сфера	
17. Прекращение или нарушение функционирования объекта информатизации, обеспечения функционирования производства и (или) технологических процессов при осуществлении деятельности, отнесенной к экологически опасной деятельности согласно приложению к Указу Президента Республики Беларусь от 24 июня 2008 г. № 349 «О критериях отнесения хозяйственной и иной деятельности, которая оказывает вредное воздействие на окружающую среду, к экологически опасной деятельности»	Вредное воздействие на окружающую среду и (или) ущерб (в том числе с учетом средств, затраченных на ликвидацию последствий) составляют более 10 тыс. базовых величин либо оказывается воздействие, выраженное в существовании угрозы здоровью или гибели людей или приводящее к гибели объектов животного или растительного мира (количество объектов, подвергшихся вредному воздействию, – более 100; количество людей, подвергшихся угрозе здоровью или гибели, – более 100; продолжительность вредного воздействия – более 12 часов)

Также следует иметь в виду, что государственные органы, уполномоченные принимать решения об отнесении объектов информатизации к критически важным, вправе самостоятельно инициировать вопрос о соответствии (несоответствии) объектов информатизации данным критериям и показателям и принимать решение об отнесении.

Таковыми государственными органами являются:

государственные органы (за исключением облисполкомов и Минского горисполкома) – в отношении объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении подчиненных этому государственному органу (входящих в его состав, систему) организаций, а также хозяйственных обществ, акции (доли в уставных фондах) которых переданы в управление этого государственного органа либо находятся в хозяйственном ведении

или оперативном управлении подчиненных этому государственному органу (входящих в его состав, систему) организаций;

облисполкомы или Минский горисполком – в отношении объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении организаций, имущество, акции (доли в уставных фондах) которых находятся в собственности соответствующей области, г.Минска, административно-территориальных единиц, входящих в состав территории этой области, г.Минска, а также объектов информатизации, находящихся в собственности, хозяйственном ведении или оперативном управлении иных организаций, не указанных в абзаце втором настоящей части, с местонахождением на территории соответствующей области, г.Минска.

Владельцы КВОИ обязаны провести ряд мероприятий по ТКЗИ, обрабатываемой на таких объектах. В частности, в течение шести месяцев со дня принятия решения об отнесении объекта информатизации к критически важным владельцы КВОИ осуществляют проектирование и создание системы информационной безопасности, под которой понимается совокупность правовых, организационных и технических мер, направленных на обеспечение информационной безопасности КВОИ (пункт 13 Положения об отнесении ОИ к КВОИ).

Особенности защиты информации, обрабатываемой на КВОИ, определены в Положении о порядке ТКЗИ. В указанном положении описаны задачи системы информационной безопасности КВОИ, функционал подразделения защиты информации (должностного лица), требования по определению порядка и правил функционирования системы информационной безопасности КВОИ, необходимые организационные и технические меры, которые должны быть реализованы в системе информационной безопасности КВОИ в зависимости от присущих ему угроз информационной безопасности КВОИ и др.

В частности, определено, что система информационной безопасности должна обеспечивать:

предотвращение неправомерного доступа к информации, обрабатываемой на КВОИ, уничтожения такой информации, ее модификации, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

обнаружение и предупреждение угроз информационной безопасности КВОИ и принятие мер по предупреждению и уменьшению рисков информационной безопасности;

недопущение реализации угроз информационной безопасности в отношении активов КВОИ, а также восстановление функционирования

КВОИ в случае такого воздействия, в том числе за счет создания и хранения резервных копий информации.

Владелец КВОИ организует и контролирует функционирование системы информационной безопасности, определяет ее состав и структуру, функции ее участников при обеспечении информационной безопасности КВОИ в зависимости от количества таких объектов и (или) особенностей деятельности владельца КВОИ.

Для проведения работ по ТКЗИ, обрабатываемой на КВОИ, владелец такого объекта создает подразделение защиты информации или назначает уполномоченное должностное лицо (далее – подразделение защиты информации (должностное лицо)). Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам ТКЗИ в порядке, установленном законодательством.

В случае невозможности выполнения силами подразделения защиты информации (должностным лицом) работ по ТКЗИ, обрабатываемой на КВОИ, руководителем организации могут привлекаться специализированные организации.

Подразделение защиты информации (должностное лицо):

разрабатывает проекты локальных правовых актов по созданию и совершенствованию системы информационной безопасности;

проводит анализ угроз и расчет рисков информационной безопасности КВОИ;

обеспечивает в соответствии с требованиями по информационной безопасности КВОИ реализацию необходимых организационных и технических мер, а также применение и эксплуатацию средств защиты информации;

осуществляет мониторинг и реагирование на возникновение рисков информационной безопасности КВОИ;

организует проведение аудита системы информационной безопасности;

согласовывает прием на работу, увольнение, перевод, перемещение работников, трудовые обязанности которых предусматривают эксплуатацию активов КВОИ, с учетом требований по информационной безопасности КВОИ;

проводит инструктажи, мероприятия по информированию и выработке практических навыков действий по обеспечению информационной безопасности КВОИ;

обеспечивает защиту сведений, содержащихся в эксплуатационной документации на КВОИ, документации на систему информационной

безопасности, иной информации, распространение и (или) предоставление которой ограничено, от ее разглашения или несанкционированного доступа к ней со стороны третьих лиц;

обеспечивает взаимодействие владельца КВОИ с юридическими и физическими лицами при заключении и исполнении договоров по вопросам обеспечения информационной безопасности КВОИ.

Обязанности, возлагаемые на подразделение защиты информации (должностное лицо), должны быть определены в локальных правовых актах владельца КВОИ. Не допускается возложение на подразделение защиты информации (должностное лицо) функций, не связанных с обеспечением ТКЗИ.

Подразделение защиты информации (должностное лицо) реализует функции, описанные выше, во взаимодействии с иными подразделениями (работниками), обеспечивающими функционирование и эксплуатацию активов КВОИ.

Объем задач, возлагаемых на подразделения (работников), обеспечивающие функционирование и эксплуатацию активов КВОИ, определяется владельцем КВОИ в локальных правовых актах по вопросам ТКЗИ, обрабатываемой на КВОИ.

Положения локальных правовых актов по вопросам ТКЗИ, обрабатываемой на КВОИ, доводятся до сведения работников, обеспечивающих функционирование и эксплуатацию активов КВОИ, в части, их касающейся.

Владельцы КВОИ не реже одного раза в год обеспечивают проведение мероприятий, направленных на повышение уровня знаний работников по вопросам информационной безопасности КВОИ, информирование о возможных рисках и угрозах информационной безопасности КВОИ.

Представители организаций, привлекаемых владельцем КВОИ для выполнения работ на таких объектах, должны быть ознакомлены с требованиями локальных правовых актов по вопросам ТКЗИ, обрабатываемой на КВОИ, в части, их касающейся.

При осуществлении ТКЗИ, обрабатываемой на КВОИ, используются средства ТКЗИ, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

Параметры и характеристики применяемых средств защиты информации должны реализовывать технические меры по обеспечению информационной безопасности КВОИ.

Применяемые средства защиты информации должны быть обеспечены гарантийной и технической поддержкой со стороны

изготовителей (разработчиков) этих средств. При выборе средств защиты информации должно учитываться возможное наличие ограничений со стороны изготовителей (разработчиков) или иных лиц на применение таких средств на любом из КВОИ, принадлежащих владельцу данных объектов.

Порядок применения средств защиты информации определяется в локальных правовых актах по вопросам ТКЗИ, обрабатываемой на КВОИ.

В локальных правовых актах по вопросам ТКЗИ, обрабатываемой на КВОИ, должны быть также определены порядок и правила функционирования системы информационной безопасности, в том числе:

цели и задачи обеспечения информационной безопасности КВОИ, перечень основных угроз и нарушителей информационной безопасности КВОИ, основные организационные и технические меры, проводимые владельцем КВОИ, состав и структура системы информационной безопасности, функции ее участников, порядок применения, форма и порядок проведения аудита;

направления информационной безопасности КВОИ (политика информационной безопасности, формуляр, реестр активов КВОИ, методика оценки рисков, план обработки рисков и другое);

план мероприятий, направленных на повышение уровня знаний работников по вопросам обеспечения информационной безопасности КВОИ и информирование о возможных рисках и угрозах информационной безопасности КВОИ;

порядок реализации организационных и технических мер по обеспечению информационной безопасности КВОИ;

порядок реагирования на возникновение рисков информационной безопасности КВОИ;

порядок взаимодействия подразделений (работников) владельца КВОИ при решении задач обеспечения информационной безопасности КВОИ.

Состав и виды локальных правовых актов по вопросам ТКЗИ, обрабатываемой на КВОИ, определяются его владельцем с учетом особенностей его деятельности.

Комплекс мероприятий по ТКЗИ, обрабатываемой на КВОИ, включает проектирование, создание и аудит системы информационной безопасности.

2.3.1. Проектирование системы информационной безопасности

На этапе проектирования системы информационной безопасности осуществляются:

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

определение целей обеспечения информационной безопасности КВОИ, совместимых с процессами деятельности владельца КВОИ и прогнозными документами организации;

инвентаризация (выявление и учет), а также определение степени важности для основной деятельности владельца КВОИ (исходя из конфиденциальности, целостности и доступности) следующих активов КВОИ:

программно-аппаратных средств и физических устройств;

программного обеспечения (прикладного и системного);

средств защиты информации;

ИС и информационных сетей;

средств обработки информации (потоков информации), средств коммуникации, администрирования и конфигурирования;

определение работников, ответственных за использование активов КВОИ;

определение физических и логических границ области применения системы информационной безопасности (формуляр КВОИ) с использованием структурной и логической схем КВОИ. При этом структурная схема должна содержать расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированных рабочих мест администратора (оператора). В логической схеме должны быть отображены ИС, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств;

определение угроз информационной безопасности КВОИ;

разработка методологии (методики) оценки рисков информационной безопасности КВОИ и оценка таких рисков;

определение требований к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, по обеспечению информационной безопасности КВОИ, блокированию (нейтрализации) угроз информационной безопасности КВОИ;

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

2.3.2. Создание системы информационной безопасности

При создании системы информационной безопасности учитывается ее информационное взаимодействие с иными ИС, автоматизированными системами управления технологическими процессами или информационно-телекоммуникационными сетями.

Обеспечение информационной безопасности КВОИ достигается путем выполнения совокупности правовых, организационных и технических мер, направленных на блокирование (нейтрализацию) угроз информационной безопасности КВОИ, реализация которых может привести к прекращению или нарушению функционирования такого объекта, обеспечиваемого (управляемого, контролируемого) им процесса, нарушению конфиденциальности, целостности, доступности обрабатываемой информации.

Меры по обеспечению информационной безопасности КВОИ определяются и реализуются с учетом угроз информационной безопасности КВОИ на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации.

В ходе создания системы информационной безопасности осуществляется разработка политики информационной безопасности КВОИ, которая содержит:

- приоритетные направления информационной безопасности КВОИ;
- перечень требований по информационной безопасности КВОИ и обязательства сотрудников по их выполнению;
- организационную структуру системы информационной безопасности;
- обязательства по постоянному совершенствованию системы информационной безопасности и выполнению актов законодательства по вопросам ТКЗИ, локальных правовых актов.

В системе информационной безопасности в зависимости от угроз информационной безопасности КВОИ реализуются следующие организационные и технические меры:

- идентификация и аутентификация:
 - определение политик и процедур идентификации и аутентификации;
 - идентификация и аутентификация пользователей и инициируемых ими процессов;
 - инвентаризация и контроль за активами КВОИ;
- управление доступом к активам КВОИ:
 - определение политик и процедур управления доступом;
 - разделение прав доступа пользователей;
 - управление учетными записями и паролями пользователей;
 - управление привилегированными правами доступа;

ограничение неуспешных попыток доступа к активам КВОИ;
оповещение пользователя при входе о предыдущем доступе к активам КВОИ;
ограничение числа параллельных сеансов доступа;
блокирование сеанса доступа пользователя при неактивности;
ограничение защищенного удаленного доступа к активам КВОИ;
контроль доступа из внешних ИС;
использование выделенного автоматизированного рабочего места для администрирования, требующего привилегированного доступа, не имеющего доступа к внешним информационным сетям;
управление запуском, установкой (инсталляцией) компонентов программного обеспечения (приложений);
– обращение с носителями информации:
определение политик и процедур обращения со съемными носителями информации;
учет съемных носителей информации;
управление физическим доступом к съемным носителям информации;
контроль за перемещением съемных носителей информации за пределы контролируемой зоны;
ограничение ввода (вывода) информации на периферийные устройства, в том числе съемные носители информации;
регистрация и контроль за подключением съемных носителей информации;
уничтожение (удаление) информации со съемных носителей информации;
– аудит информационной безопасности:
определение политик и процедур аудита информационной безопасности;
поиск уязвимостей активов КВОИ и их устранение;
генерирование временных меток и (или) синхронизация системного времени;
защита информации о событиях информационной безопасности;
аудит информации о действиях пользователей;
регистрация и мониторинг событий информационной безопасности;
хранение результатов аудита безопасности;
защита от ВПО;
определение политик и процедур защиты от ВПО;
реализация защиты от ВПО;
обновление механизмов сканирования и базы данных сигнатур ВПО;
регистрация событий обнаружения вредоносных программ;
– управление процедурами резервирования:

определение политик и процедур резервирования;
резервирование программных и программно-аппаратных средств и систем;
резервное копирование информации, программного обеспечения и обеспечение возможности восстановления из резервных копий;
резервное копирование конфигурационных файлов и журналов аудита;
обеспечение защиты резервных копий;
– обеспечение информационной безопасности КВОИ и его элементов:
определение политик и процедур защиты ИС и ее элементов;
разделение функций по управлению активами КВОИ с другими функциями;
сегментирование сети КВОИ;
управление сетевыми потоками;
использование межсетевых экранов;
сокрытие архитектуры и конфигурации КВОИ;
управление безопасной настройкой сетевых устройств (средств защиты информации);
отключение беспроводных соединений и интерфейсов;
исключение доступа через общие ресурсы;
защита от угроз отказа в обслуживании;
ограничение использования мобильных устройств;
управление перемещением виртуальных машин и обрабатываемых на них данных;
– управление конфигурацией:
определение политик и процедур управления конфигурацией ИС;
идентификация объектов управления конфигурацией;
управление изменениями конфигурации;
установка (инсталляция) только разрешенного к использованию программного обеспечения;
контроль за действиями по изменению конфигурации;
– обновление программного обеспечения:
определение политик и процедур управления обновлениями программного обеспечения;
обновление программного обеспечения из доверенного источника;
– планирование мероприятий по обеспечению информационной безопасности КВОИ:
определение политик и процедур планирования мероприятий по обеспечению информационной безопасности КВОИ;
разработка, утверждение и актуализация плана мероприятий по обеспечению информационной безопасности КВОИ;

контроль за выполнением мероприятий по обеспечению информационной безопасности КВОИ;

– реагирование на события информационной безопасности КВОИ и управление ими:

разработка плана реагирования на события информационной безопасности и его актуализация не реже одного раза в год;

определение периодичности проведения мероприятий по оповещению и отработке действий работников в случае реализации угроз информационной безопасности КВОИ в соответствии с планом реагирования;

разработка и внедрение методологии реагирования на события информационной безопасности, обеспечивающей реагирование в сроки, определенные эксплуатационной документацией на КВОИ и локальными правовыми актами, в целях исключения (снижения до приемлемого уровня) вероятного ущерба;

обучение и отработка действий персонала при возникновении событий информационной безопасности;

создание альтернативных мест хранения и обработки информации в случае возникновения событий информационной безопасности;

анализ возникших событий информационной безопасности и принятие мер по недопущению их повторного возникновения;

– информирование и обучение персонала:

определение политик и процедур информирования и обучения персонала, ответственности за нарушение требований по информационной безопасности КВОИ;

информирование персонала об угрозах информационной безопасности КВОИ, правилах безопасной работы с активами КВОИ;

проведение практических занятий с персоналом по правилам безопасной работы;

контроль осведомленности персонала об угрозах информационной безопасности КВОИ и о правилах безопасной работы.

В целях постоянного мониторинга угроз безопасности КВОИ владелец такого объекта:

осуществляет постоянный контроль за состоянием активов КВОИ для выявления потенциальных событий информационной безопасности КВОИ;

проводит анализ и оценку угроз информационной безопасности КВОИ;

разрабатывает план восстановления КВОИ, учитывающий события информационной безопасности.

В целях определения соответствия системы информационной безопасности требованиям законодательства, в том числе обязательных

для соблюдения требований технических нормативных правовых актов в сфере ТКЗИ, проводится ее аудит. Такой аудит проводится владельцем КВОИ или специализированной организацией не позднее чем через год после завершения мероприятий по созданию системы информационной безопасности и далее ежегодно.

2.3.3. Аудит системы информационной безопасности

Аудит системы информационной безопасности включает следующие этапы:

анализ и оценку соответствия системы информационной безопасности требованиям законодательства;

проведение контроля эффективности защищенности системы информационной безопасности;

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

составление акта по форме и рекомендаций по результатам аудита.

Акт аудита системы информационной безопасности утверждается:

руководителем владельца КВОИ — в случае проведения аудита системы информационной безопасности подразделением защиты информации (должностным лицом);

руководителем специализированной организации — в случае проведения аудита данной организацией.

Форма

Для служебного пользования
Экз. № ____

УТВЕРЖДАЮ

Руководитель организации

Фамилия, инициалы

____.____.20____

АКТ

аудита системы информационной безопасности критически важного объекта информатизации

(наименование критически важного объекта информатизации)

Вопросы, подлежащие рассмотрению	Отметка о выполнении, номер, дата, наименование документа, в котором реализованы требования
Разработка политики информационной безопасности критически важного объекта информатизации (далее – КВОИ)	
Проведение инвентаризации (выявление и учет) активов КВОИ	
Определение работников, ответственных за использование активов КВОИ	
Определение физических и логических границ области применения системы информационной безопасности	
Определение угроз информационной безопасности КВОИ	
Разработка методологии (методики) оценки рисков информационной безопасности КВОИ	
Оценка рисков информационной безопасности КВОИ	
Определение требований к параметрам настройки программных и программно-аппаратных средств, средств защиты информации	
Определение средств управления, необходимых для реализации выбранного варианта обработки рисков безопасности КВОИ (план обработки рисков)	
Идентификация и аутентификация	
Управление доступом к активам КВОИ	
Обращение с носителями информации	
Аудит информационной безопасности	
Защита от вредоносного программного обеспечения	
Управление процедурами резервирования	
Обеспечение информационной безопасности КВОИ и его элементов	
Управление конфигурацией	
Обновление программного обеспечения	
Планирование мероприятий по обеспечению информационной безопасности КВОИ	
Реагирование на события информационной безопасности КВОИ и управление ими	
Информирование и обучение персонала	
Осуществление постоянного контроля за состоянием активов КВОИ в целях выявления событий информационной безопасности КВОИ	
Анализ и оценка угроз информационной безопасности КВОИ	
Разработка плана восстановления КВОИ	

Председатель комиссии

(подпись)

(инициалы, фамилия)

Члены комиссии:

(подпись)

(инициалы, фамилия)

(подпись)

(инициалы, фамилия)

Государственным органам и организациям необходимо учитывать, что согласно пунктам 13 – 15 перечня сведений, относящихся к служебной информации ограниченного распространения, определенного

постановлением № 783, отдельные виды информации о КВОИ относятся к служебной информации ограниченного распространения, а именно:

совокупность сведений об объекте информатизации, включенном в государственный реестр КВОИ;

сведения о системе информационной безопасности КВОИ;

сведения, полученные в результате проведения аудита системы информационной безопасности КВОИ и контроля за ТКЗИ на КВОИ.

2.4. Обязательные требования по безопасности использования национального сегмента сети Интернет

Согласно пункту 4 Указа Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» государственные организации обязаны размещать существующие, создаваемые (приобретаемые, модернизируемые) программно-технические средства, ИС (ресурсы) на ресурсах республиканского центра обработки данных (далее – РЦОД) и (или) республиканской платформы (далее – РП), за исключением случаев, установленных законодательством.

Размещение существующих программно-технических средств, ИС (ресурсов) государственных организаций на ресурсах РЦОД и (или) РП осуществляется поэтапно на основании планов-графиков. Так, например, соответствующий план-график на 2024 год утвержден постановлением Совета Министров Республики Беларусь от 21 июня 2023 г. № 397.

ИС (ресурсы) государственных организаций, интегрированные с общегосударственной автоматизированной информационной системой (далее – ОАИС), и соответствующие программно-технические средства размещаются на ресурсах РЦОД и (или) РП либо на информационно-коммуникационной инфраструктуре республиканского унитарного предприятия «Национальный центр электронных услуг» (далее – оператор ОАИС), в том числе с применением программно-аппаратного комплекса динамической доверенной среды.

ИС (ресурсы) и программно-технические средства, принадлежащие организациям частной формы собственности, физическим лицам, в том числе индивидуальным предпринимателям, размещаются на ресурсах РЦОД и (или) РП по желанию их владельцев (собственников).

Не подлежат размещению на ресурсах РЦОД и (или) РП программно-технические средства, ИС (ресурсы) государственных организаций:

предназначенные для обработки информации, отнесенной к государственным секретам;

используемые для осуществления особого контроля в сфере предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;

в иных случаях, предусмотренных Президентом Республики Беларусь.

ИС (ресурсы), оператором которых является оператор ОАИС, ИС (ресурсы), в отношении которых их владельцами (собственниками) принято решение о нецелесообразности их размещения на ресурсах РЦОД и (или) РП, и соответствующие программно-технические средства размещаются на данных ресурсах по желанию их владельцев (собственников).

Такое решение принимается на основании Методики оценки и принятия решения о целесообразности размещения существующих, создаваемых (приобретаемых, модернизируемых) программно-технических средств, информационных систем (ресурсов) государственных организаций на ресурсах республиканского центра обработки данных и (или) республиканской платформы, утвержденной постановлением Совета Министров Республики Беларусь от 31 марта 2021 г. № 182 «О мерах по реализации Указа Президента Республики Беларусь от 16 декабря 2019 г. № 461».

В случае принятия такого решения государственной организации предоставляется два альтернативных решения по вопросу выбора используемой ИИ:

использование собственной ИИ;

приобретение интернет-услуг у уполномоченных поставщиков интернет-услуг (хостинг официальных интернет-сайтов и электронной почты, имеющей подключение к сети Интернет (далее – электронная почта) или иных организаций (для хостинга иных ресурсов, размещения на ИИ поставщика интернет-услуг ОИИ государственных организаций, не обеспечивающих функционирование официальных интернет-сайтов и (или) электронной почты).

Институт уполномоченных поставщиков интернет-услуг введен в действие пунктом 7 Указа № 60.

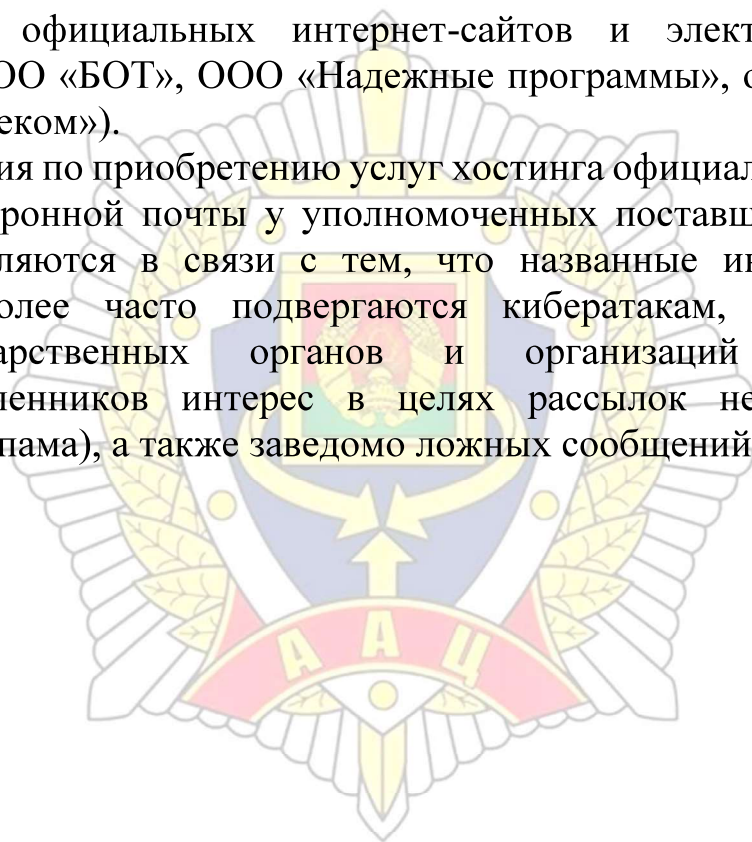
Положение о порядке определения уполномоченных поставщиков интернет-услуг (вместе с требованиями, которые предъявляются к таким поставщикам) утверждено приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г. № 60.

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2010 г. № 92 определены поставщики интернет-услуг, уполномоченные оказывать услуги по предоставлению:

доступа к сети Интернет (государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси», государственное учреждение «Главное хозяйственное управление» Управления делами Президента Республики Беларусь (далее – ГУ «ГХУ»), закрытое акционерное общество «ГлобалВанБел», общество с ограниченной ответственностью (далее – ООО) «АйПи ТелКом», ООО «Белорусские облачные технологии» (далее – ООО «БОТ»), ООО «Деловая сеть», республиканское унитарное предприятие электросвязи (далее – РУП) «Белтелеком», совместное общество с ограниченной ответственностью (далее – СООО) «КОСМОС ТВ», СООО «Мобильные ТелеСистемы» и унитарное предприятие по оказанию услуг «А1»);

хостинга официальных интернет-сайтов и электронной почты (ГУ «ГХУ», ООО «БОТ», ООО «Надежные программы», оператор ОАИС и РУП «Белтелеком»).

Требования по приобретению услуг хостинга официальных интернет-сайтов и электронной почты у уполномоченных поставщиков интернет-услуг предъявляются в связи с тем, что названные информационные ресурсы наиболее часто подвергаются кибератакам, а электронная почта государственных органов и организаций представляет для злоумышленников интерес в целях рассылки незапрашиваемой информации (спама), а также заведомо ложных сообщений об опасности.



3. МОНИТОРИНГ КИБЕРБЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ

Постановлением Совета Министров Республики Беларусь от 23 февраля 2024 г. № 120 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (далее – постановление Правительства № 120) определен 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.

Государственным органам и организациям следует учитывать, что данный перечень подлежит ежегодной актуализации согласно подпункту 3.4 пункта 3 Указа № 40.

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

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

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

С учетом изложенного, для исключения проблемных аспектов при формировании соответствующих бюджетов государственным органам и организациям следует ответственно подходить к вопросу представления сведений, подлежащих включению в финансово-экономическое обоснование к проекту постановления Правительства.

Руководители государственных органов и иных организаций, включенных в перечень из постановления Правительства № 120 в соответствии с требованиями подпункта 3.15 пункта 3 Указа № 40 назначают одного из своих заместителей ответственным за организацию работы по обеспечению кибербезопасности этого органа (организации), в том числе за осуществление мероприятий по обнаружению,

предотвращению и минимизации последствий кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты.

Вместе с тем руководителям государственных органов и организаций рекомендуется назначить такое должностное лицо и в том случае, если возглавляемая ими организация еще не включена в соответствующий перечень.

Права и обязанности такого заместителя руководителя определяются руководителем этого органа (организации) с учетом рекомендаций ОАЦ, размещенных на официальном интернет-сайте ОАЦ.

Решение о выборе варианта реализации указанного требования, определенного постановлением Правительства № 120 (создание центра кибербезопасности или приобретение услуг), зависит от множества факторов и принимается руководством соответствующих организаций самостоятельно.

3.1 Создание центров кибербезопасности

Указом № 40 предусмотрено, что центры кибербезопасности:

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

проводят оценку степени защищенности ОИИ, мероприятия по установлению причин киберинцидентов, вызванных кибератаками на ОИИ;

осуществляют сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на ОИИ;

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

обеспечивают функционирование в своем составе команд реагирования на киберинциденты.

При создании таких центров необходимо опираться на три основных взаимосвязанных блока, которые не в силах работать по отдельности: процессы, люди, технологии (технические, программно-аппаратные и программные средства, в том числе средства защиты информации). Их и предлагается рассмотреть.

Точный перечень процессов, необходимых для выполнения центром кибербезопасности возлагаемых на него задач, зависит от подключенных к нему ОИИ. В то же время, можно выделить некоторые основные группы универсальных процессов, в том числе таких как:

- работа с подключенными ОИИ;

- выявление инцидентов / мониторинг;

- реагирование на инциденты, их расследование / выявление причин;

Применительно к составу средств, которые должны находиться в собственности или на ином законном основании, центра кибербезопасности, последние должны использовать в том числе средства:

- 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);

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

Наконец, любые материальные вложения в технические, программно-аппаратные и программные средства, в том числе средства защиты информации, будут малоэффективными или даже бессмысленными, если их будет обслуживать недостаточное количество персонала, и, что еще хуже, не обладающего необходимой для этого квалификацией.

Учитывая изложенное, типовая структура центра кибербезопасности должна предусматривать наличие структурных подразделений (единиц):

- руководителя центра кибербезопасности;

- структурного подразделения, выполняющего функции по автоматизированному сбору сведений о событиях информационной безопасности и данных о киберинцидентах;

- структурного подразделения, выполняющего функции по администрированию автоматизированной системы взаимодействия;

- структурного подразделения, выполняющего функции команды реагирования на киберинциденты;

- структурного подразделения или лица, ответственного за обеспечение кибербезопасности;

- структурного подразделения или лица, выполняющего функции по анализу вредоносных программ;

- структурного подразделения или лица, выполняющего функции по оценке степени защищенности (тестирование на проникновение) ОИИ.

При этом допускается привлечение к работе центра кибербезопасности по функционалу последних двух структурных подразделений или лиц сторонних организаций или физических лиц на

основании гражданско-правовых договоров. В данном случае создание таких структурных подразделений или наличие в штате соответствующих лиц не требуется.

Конкретные требования к центрам кибербезопасности, которым последние должны соответствовать для прохождения их аттестации регламентированы Приложением 2 к приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (далее – приказ ОАЦ № 130).

В целом, при принятии решения о создании собственного центра кибербезопасности следует учитывать следующие факторы

для построения результативного центра кибербезопасности требуется применять целый ряд обязательных технологий (средства выявления и реагирования на киберинциденты (система сбора и обработки событий информационной безопасности (SIEM); платформы управления информацией об угрозах (Threat Intelligence Platform); средства динамического анализа вредоносных программ типа «песочница», средства аудита информационной безопасности и оценки эффективности защищенности (средств тестирования на проникновение) (сетевой сканер; сканер уязвимостей; сканер уязвимостей веб-приложений) и т.д.) Эти средства защиты информации играют наиважнейшую роль в обеспечении безопасности объектов информационной инфраструктуры и эффективной работе центра кибербезопасности. Их использование помогает обнаруживать и предотвращать продвинутое киберугрозы, защищать конечные точки от вредоносных программ, контролировать передачу и использование конфиденциальной информации. Реализация этих средств в составе центра кибербезопасности помогает обеспечить комплексную защиту объектов информационной инфраструктуры государственных органов и иных организаций. В то же время, следует учитывать, что перечень решений, предусмотренных в соответствующем приказе, не является исчерпывающим и лишь описывает минимально необходимый комплект инструментов, необходимым для эффективной борьбы с современными угрозами кибербезопасности;

эффективное выполнение задач, возложенных на центры кибербезопасности, требует реализации ряда важных процессов. Эти процессы, такие как бесперебойное функционирование и восстановление работоспособности автоматизированной системы взаимодействия, синхронизация системного времени от единого (общего) источника и т.д., играют ключевую роль в обеспечении безопасности объектов информационной инфраструктуры государственных органов и иных организаций, а также содержащейся в них информации. Однако, помимо практической реализации, важно также документально оформить

регламенты этих процессов. Это способствует зрелости этих процессов, минимизирует влияние конкретных личностей и обеспечивает возможность быстрой адаптации новых сотрудников к текущим задачам. Документирование регламентов также сокращает время на решение задач, повышает эффективность работы и обеспечивает стабильность в деятельности центра кибербезопасности;

результативность центров кибербезопасности зависит не только от внедрения современных технологий и процессов, но и от квалификации и профессионализма специалистов, работающих в этих центрах. Постоянно изменяющийся ландшафт киберугроз требует наличия квалифицированных сотрудников в области кибербезопасности, в связи с чем вопросам обучения следует уделять первостепенное внимание. Надлежащая подготовка, непрерывное профессиональное развитие, правовая и этическая осведомленность являются жизненно важными компонентами создания и поддержания высококвалифицированной и эффективной команды, обеспечивающей надлежащий уровень кибербезопасности в масштабах государства. В этой связи важно обеспечить их непрерывное обучение и развитие, а также формирование четких регламентов и процедур, что способствует зрелости процессов, минимизирует влияние человеческого фактора и позволяет новым сотрудникам быстро адаптироваться и эффективно выполнять поставленные задачи.

3.2 Приобретение услуг по обеспечению кибербезопасности

Перечень организаций, у которых государственные органы и иные государственные организации вправе приобретать услуги по обеспечению кибербезопасности с применением процедуры закупки из одного источника, определенный постановлением Правительства № 120, формируется по принципу включения в него всех организаций, в которых созданные центры кибербезопасности прошли процедуру аттестации (и которые планируют оказывать услуги по обеспечению кибербезопасности).

Полные же перечень таких центров размещен на официальном интернет-сайте ОАЦ по ссылке: <https://www.oac.gov.by/activity/cybersecurity-centers-list/certified-cybersecurity-centers>.

Государственным органам и организациям следует учитывать, что центры кибербезопасности до начала оказания услуг по обеспечению кибербезопасности обязаны:

разработать по каждому ОИИ регламент обеспечения кибербезопасности ОИИ (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;

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.

В регламенте указывается следующая информация:

наименование ОИИ;

собственник (владелец) ОИИ (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей);

место нахождения ОИИ;

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;

контактный номер телефона, адрес электронной почты работника, ответственного за функционирование ОИИ, либо контактный номер телефона дежурной смены (при наличии);

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

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;

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

структурная схема ОИИ (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);

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

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

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.

Договоры же на оказание услуг по обеспечению кибербезопасности ОИИ должны содержать:

в качестве существенных условий:

обязательства сторон по разработке по каждому ОИИ соответствующих регламентов;

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

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;

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

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

Копия договора направляется в ОАЦ в течение пяти рабочих дней со дня его заключения (часть первая подпункта 3.10 пункта 3 Указа № 40).

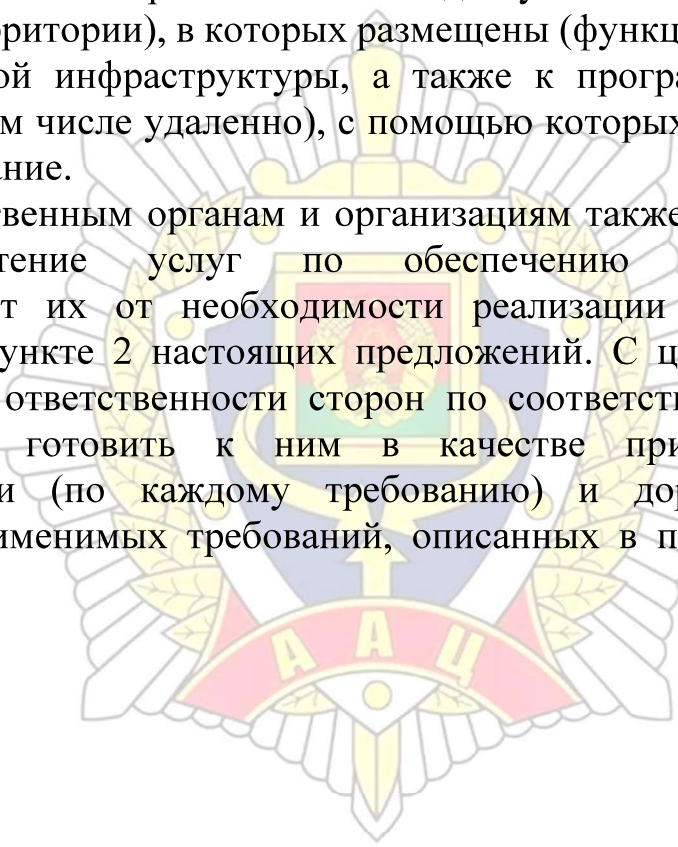
Также следует учитывать, что согласно подпункту 3.3 пункта 3 Указа № 40 при обеспечении кибербезопасности ОИИ, в том числе реализации мероприятий по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов, реагированию на такие

киберинциденты, уполномоченные лица центров кибербезопасности обладают правом требовать от государственных органов и организаций, которым они оказывают соответствующие услуги (если данные права определены в договоре на оказание услуг по обеспечению кибербезопасности):

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

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

Государственным органам и организациям также следует понимать, что приобретение услуг по обеспечению кибербезопасности не освобождает их от необходимости реализации иных требований, описанных в пункте 2 настоящих предложений. С целью однозначного распределения ответственности сторон по соответствующим договорам рекомендуется готовить к ним в качестве приложения матрицу ответственности (по каждому требованию) и дорожную карту по реализации применимых требований, описанных в пункте 2 настоящих предложений.



4. ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ С ОАЦ

По состоянию на 1 сентября 2024 г. информационное взаимодействие по вопросам обеспечения состояния защищенности информационной инфраструктуры и обрабатываемой в ней информации от внутренних и внешних угроз можно разделить на две дополняющие друг друга составляющие:

информационное взаимодействие вне Национальной системы обеспечения кибербезопасности;

информационное взаимодействие в Национальной системе обеспечения кибербезопасности.

4.1 Информационное взаимодействие вне Национальной системы обеспечения кибербезопасности

Согласно Положению о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации, утвержденному приказом ОАЦ № 66 государственные органы и организации представляют в ОАЦ следующие сведения:

– сведения о событиях информационной безопасности, в том числе о фактах возникновения угроз информационной безопасности КВОИ:

описание источника угрозы информационной безопасности критически важного объекта информатизации и активов критически важного объекта информатизации, на которые она направлена;

условия и причины возникновения угроз информационной безопасности критически важного объекта информатизации.

Такие сведения представляются в произвольной форме в течение суток с момента выявления (обнаружения) соответствующих фактов;

– сведения об ИС, предназначенных для обработки ИРиПКО и о подразделениях защиты информации или иных подразделениях (должностных лицах), ответственных за обеспечение защиты информации.

Такие сведения представляются ежегодно до 1 февраля года, следующего за отчетным, посредством общегосударственной автоматизированной информационной системы (коды услуг единого портала электронных услуг 3.08.01 и 3.08.02);

– копии аттестата соответствия системы защиты информации ИС требованиям по защите информации, технического отчета и протокола испытаний.

Такие сведения представляются не позднее десяти календарных дней со дня оформления (получения) аттестата соответствия системы защиты информации ИС требованиям по защите информации;

– формуляр КВОИ – не позднее пяти рабочих дней после завершения мероприятий по созданию системы информационной безопасности КВОИ и (или) изменения сведений, указанных в формуляре;

– результаты аудита системы информационной безопасности КВОИ – не позднее чем через год после завершения мероприятий по созданию системы информационной безопасности КВОИ и далее ежегодно.

4.2 Информационное взаимодействие в Национальной системе обеспечения кибербезопасности

Порядок информационного взаимодействия элементов национальной системы обеспечения кибербезопасности определен в одноименном Положении, утвержденном приказом ОАЦ № 130.

Информационное взаимодействие осуществляется в целях:

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

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 ОИИ;

информирования государственных органов и иных организаций об угрозах в отношении принадлежащих им ОИИ 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 ОИИ;

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

Информационное взаимодействие осуществляется с использованием автоматизированных систем взаимодействия, т.е. информационных систем государственных органов и иных организаций, предназначенных 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.

При этом, согласно Закону № 455-З под ИС следует совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

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.

Таким образом, любой из указанных способов является официальным и, например, может использоваться уполномоченными лицами Национального центра кибербезопасности для формирования требований государственным органам и иным организациям в части:

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

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

При этом при выявлении нарушений положений Указа № 40 и иных актов законодательства, принятых в его развитие (в том числе приказа № 130) ОАЦ вправе выносить государственным органам и организациям обязательные для исполнения предписания.

4.3 Особенности информационного взаимодействия с центрами кибербезопасности

При осуществлении информационного взаимодействия 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 (технические сведения, которые фактически или потенциально могут свидетельствовать о компрометации, попытках компрометации или иного вредоносного воздействия на объекты информационной инфраструктуры) 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 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.

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.

Сведения о событиях информационной безопасности, подлежащие сбору, обработке и хранению центром кибербезопасности, должны соответствовать перечню 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.

4.4 Обмен информацией с иностранными и международными организациями

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.

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

5. ФУНКЦИОНИРОВАНИЕ НАЦИОНАЛЬНОЙ КОМАНДЫ РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ (CERT.BY), КОМАНД РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ ЦЕНТРОВ КИБЕРБЕЗОПАСНОСТИ

Отношения, связанные с порядком функционирования национальной команды реагирования на киберинциденты (CERT.BY), команд реагирования на киберинциденты центров кибербезопасности регулируются соответствующим Положением, утвержденным приказом ОАЦ № 130.

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

При этом к киберинцидентам высокого уровня относятся:

- внедрение и функционирование вредоносных программ на ОИИ;
- несанкционированный доступ к ОИИ с использованием ИКТ;
- использование ОИИ для осуществления кибератак и (или) распространения вредоносных программ;
- прослушивание, захват, перенаправление сетевого трафика ОИИ;
- рассылка незапрашиваемой информации (спама) с ОИИ;
- эксплуатация уязвимостей на ОИИ;
- прекращение функционирования ОИИ, вызванное кибератакой типа «отказ в обслуживании».

Решение об участии национальной команды реагирования в ликвидации последствий киберинцидентов высокого уровня принимается руководителем Национального кибербезопасности по согласованию с начальником 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.

К киберинцидентам низкого уровня, в свою очередь, 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.

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).

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.

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.

В целях 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 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.

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.

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.

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.



6. ПЕРЕЧЕНЬ ОСНОВНЫХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».
2. Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет».
3. Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации».
4. Указ Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий».
5. Указ Президента Республики Беларусь от 14 февраля 2023 № 40 «О кибербезопасности».
6. Постановление Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)».
7. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г. № 60 «Об утверждении Положения о порядке определения уполномоченных поставщиков интернет-услуг».
8. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2010 г. № 92 «Об утверждении перечня уполномоченных поставщиков интернет-услуг».
9. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь».
10. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».
11. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 марта 2020 г. № 77 «О подтверждении соответствия средств защиты информации».
12. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40».