

**Информационные технологии и безопасность  
БЕЗОПАСНАЯ ЭКСПЛУАТАЦИЯ И НАДЕЖНОЕ  
ФУНКЦИОНИРОВАНИЕ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ  
ИНФОРМАТИЗАЦИИ  
Общие требования**

**Інфармацыйныя тэхналогіі і бяспека  
БЯСПЕЧНАЯ ЭКСПЛУАТАЦЫЯ І НАДЗЕЙНАЕ  
ФУНКЦЫЯНІРАВАННЕ КРЫТЫЧНА ВАЖНЫХ АБ'ЕКТАЎ  
ІНФАРМАТЫЗАЦЫІ  
Агульныя патрабаванні**



---

УДК

МКС 35.040

КП 05

**Ключевые слова:** информационная технология, безопасность, безопасная эксплуатация, надежное функционирование, критически важный объект информатизации, общие требования

---

### Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь "О техническом нормировании и стандартизации".

1 РАЗРАБОТАН Научно-производственным республиканским унитарным предприятием "Научно-исследовательский институт технической защиты информации" (Государственное предприятие "НИИ ТЗИ")

ВНЕСЕН Оперативно-аналитическим центром при Президенте Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от \_\_\_\_\_ № \_\_\_\_\_

3 ВВЕДЕН ВПЕРВЫЕ

Настоящий технический кодекс установившейся практики не может быть тиражирован и распространен в качестве официального издания без разрешения Госстандарта Республики Беларусь

---

Издан на русском языке

## Содержание

1 Область применения .....	1
2 Нормативные ссылки.....	1
3 Термины и определения .....	1
4 Обозначения и сокращения .....	2
5 Общие положения.....	3
6 Распределение обязанностей по обеспечению безопасности критически важных объектов информатизации.....	4
6.1 Назначение ответственного лица.....	4
6.2 Организация работы с персоналом.....	5
6.3 Организация обслуживания в процессе эксплуатации.....	6
7 Обеспечение информационной безопасности .....	7
8 Обеспечение сетевой безопасности .....	11
9 Обеспечение физической безопасности.....	13
10 Управление безопасной эксплуатацией .....	14
11 Планирование обеспечения безопасности.....	18
12 Разработка и реализация планов реагирования на инциденты .....	20
13 Разработка и реализация планов восстановления после инцидентов .....	20
14 Обеспечение надежного функционирования КВОИ в процессе эксплуатации .....	22
14.1 Обеспечение надежного функционирования КВОИ на этапах его жизненного цикла .....	22
14.2 Требования к надежности технических средств и оборудования.....	24
14.3 Требования к надежности программного обеспечения .....	25
15 Техническое обследование критически важных объектов информатизации для оценки соответствия состояния технической защиты информации установленным требованиям .....	26
16 Идентификация критически важных объектов информатизации критической инфраструктуры .....	29



**ТЕХНИЧЕСКИЙ КОДЕКС УСТАНОВИВШЕЙСЯ ПРАКТИКИ****Информационные технологии и безопасность  
БЕЗОПАСНАЯ ЭКСПЛУАТАЦИЯ И НАДЕЖНОЕ ФУНКЦИОНИРОВАНИЕ  
КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ****Общие требования****Інформаційні технології  
БЯСПЕЧНА ЕКСПЛУАТАЦІЯ І НАДЗЕЙНАЄ ФУНКЦІОНІВАННЯ  
КРИТИЧНА ВАЖНИХ ОБ'ЄКТАЇ  
Агульні патрабаванні**

Information Technology and Safety  
Safety Operation And Reliable Operation of  
Crucial Objects of Informatization  
General requirements

**Дата введения ХХ-ХХ-20ХХ****1 Область применения**

Настоящий технический кодекс установившейся практики (далее – технический кодекс) регламентирует вопросы безопасности, специфичные для объектов критических инфраструктур (КИ) критически важных объектов информатизации (КВОИ), устанавливает требования по обеспечению безопасной эксплуатации и надежного функционирования КВОИ и соответствующие им мероприятия.

Требования настоящего технического кодекса обязательны для субъектов, осуществляющих деятельность, связанную с разработкой, созданием, эксплуатацией, обслуживанием, использованием, аудитом безопасности КВОИ.

**2 Нормативные ссылки**

В настоящем техническом кодексе использованы ссылки на следующие технические нормативные правовые акты в области технического нормирования и стандартизации (далее – ТНПА):

СТБ ISO/IEC 27001-2011 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

СТБ П 34.101.39 – 2009 Информационная технология. Безопасность. Специальное программное обеспечение. Требования и методы испытаний

Примечание – При пользовании настоящим техническим кодексом целесообразно проверить действие ТНПА по каталогу, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году.

Если ссылочные ТНПА заменены (изменены), то при пользовании настоящим техническим кодексом следует руководствоваться замененными (измененными) ТНПА. Если ссылочные ТНПА отменены без замены, то положение, в котором дана ссылка на них, применяется в части, не затрагивающей эту ссылку.

**3 Термины и определения**

В настоящем техническом кодексе применяют следующие термины с соответствующими определениями:

**3.1 актив:** Все, что имеет ценность для организации (СТБ ISO/IEC 27001).

**3.2 воздействие:** Результат нежелательного инцидента [1].

**3.3 безопасность:** Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба [2].

Примечание – В области стандартизации безопасность продукции, процессов и услуг обычно рассматривается с целью достижения оптимального баланса ряда факторов, включая такие нетехнические факторы, как поведение человека, позволяющего свести устранимый риск, связанный с возможностью.

**3.4 гарантия инфраструктуры:** Уверенность в готовности, надежности и непрерывности функционирования инфраструктур, заключающаяся в том, что они в минимальной степени повреждаются в незначительной степени в случае аварии или атаки и могут быть быстро восстановлены для возобновления функционирования жизненно важного оборудования.

**3.5 инцидент безопасности:** Любое злоумышленное или подозрительное действие, о котором известно, что оно вызывает или может иметь результатом нарушение безопасности объекта критической инфраструктуры.

**3.6 критически важный объект информатизации:** Объект информатизации, нарушение (прекращение) функционирования которого может привести к чрезвычайной ситуации техногенного характера или к значительным негативным последствиям для безопасности в политической, экономической, социальной, информационной, экологической и иных сферах [3].

**3.7 критическая инфраструктура:** Инфраструктура, являющаяся жизненно важной для государства, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность [3].

**3.8 объект информатизации; ОИ:** Средства электронной вычислительной техники вместе с программным обеспечением (ПО), в том числе автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, используемые для обработки информации [3].

**3.9 оценка воздействия:** Оценка экономических, экологических, правовых и социальных последствий реализации угрозы в отношении элемента инфраструктуры.

**3.10 угроза безопасности:** Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

**3.11 уровень критичности актива:** Установление градации (категории) информации и ресурса по показателям их значимости для решения производственных задач, ущерба от потери качества или недоступности актива.

#### 4 Обозначения и сокращения

В настоящем техническом кодексе применяются следующие обозначения и сокращения:

КВОИ	– критически важный объект информатизации;
КИ	– критическая инфраструктура;
НПА	– нормативный правовой акт;
НСД	– несанкционированный доступ
ОДЛ	– ответственное должностное лицо по всем аспектам информационной безопасности критически важного объекта информатизации;
ОИ	– объект информатизации;
ПО	– программное обеспечение
СВТ	– средство вычислительной техники;
ТЗИ	– техническая защита информации;
ТТЗ	– тактико-техническое задание;
ТНПА	– технический нормативный правовой акт в области технического нормирования и стандартизации;
ТС	– техническое средство.

## 5 Общие положения

**5.1** Безопасность КВОИ достигается непосредственным применением и расширением лучших методов и способов сложившейся практики, которые базируются на подходах к обеспечению информационной безопасности, поддерживаемых НПА Республики Беларусь, национальными ТНПА, распоряжениями регулирующих органов, позволяющих учесть специфику КВОИ в различных отраслях, на мировом опыте, отраженном в международных ТНПА и руководствах.

**5.2** Безопасное функционирование КВОИ обеспечивается созданием условий его эксплуатации в соответствии с требованиями эксплуатационной и организационно-распорядительной документации, не противоречащей требованиям, установленными НПА, государственными и ведомственными ТНПА.

**5.3** Безопасная эксплуатация и надежное функционирование КВОИ должны обеспечиваться созданием комплексной системы защиты, включающей мероприятия, реализуемые с помощью:

- организационных средств защиты, включающих правила и процедуры по организации и контролю работы персонала КВОИ и безопасности предприятия в целом;
- организационно-технических средств защиты (с применением программных, программно-аппаратных, аппаратных средств и устройств), реализующих технологические способы предотвращения вторжения, перехвата и других видов несанкционированного доступа к ресурсам КВОИ, обеспечивающих целостность, доступность, конфиденциальность информации в ходе обработки данных;
- физических мер защиты с применением систем и средств, предназначенных для охраны КВОИ и защиты его компонентов от несанкционированного физического доступа и диверсий.

**5.4** Защищенность КВОИ в эксплуатации обеспечивается выполнением следующих обязательных мероприятий, предусматривающих:

- идентификацию КВОИ и ее подтверждение;
- распределение обязанностей по обеспечению безопасности КВОИ;
- обеспечение информационной безопасности КВОИ;
- обеспечение сетевой безопасности КВОИ;
- обеспечение физической безопасности КВОИ;
- управление безопасной эксплуатацией КВОИ;
- разработку и реализацию планов реагирования на инциденты безопасности КВОИ;
- разработку и реализацию планов восстановления КВОИ после инцидентов;
- обеспечение надежного функционирования КВОИ в процессе эксплуатации;
- техническое обследование КВОИ для оценки соответствия состояния ТЗИ установленным требованиям.

Мероприятия по идентификации КВОИ направлены на выявление критичных активов объектов КИ, принятия решения об отнесении ОИ к КВОИ, подтверждение корректности отнесения и поддержку актуализированного перечня КВОИ.

Мероприятия по распределению обязанностей по обеспечению безопасности КВОИ направлены на назначение ответственных лиц по всем аспектам безопасности КВОИ, организацию своевременного их обучения и повышения квалификации, ведение учетных записей, касающихся персонала, организацию безопасной работы с организациями-субподрядчиками и поставщиками товаров и услуг, связанных с безопасностью КВОИ.

Мероприятия по обеспечению информационной безопасности КВОИ направлены на создание системы защиты информации КВОИ в соответствии с требованиями НПА, ТНПА и целями безопасности объекта КИ путем разработки политики информационной безопасности, разработки и реализации требований задания по безопасности, ввода в действие организационно-распорядительной документации, аттестации системы защиты информации КВОИ, управления информационной безопасностью.

Мероприятия по обеспечению сетевой безопасности КВОИ направлены на разработку организационно-распорядительной документации, регулирующей вопросы определения и защиты электронного периметра КВОИ при взаимодействии с другими ОИ, с последующей реализацией ее положений и своевременным пересмотром.

Мероприятия по обеспечению физической безопасности КВОИ направлены на создание системы мониторинга, управления, регистрации и контроля доступа на объект КИ от несанкционированных действий в нарушение политикой информационной безопасности.

Мероприятия по управлению безопасной эксплуатацией КВОИ направлены на предотвращение рисков нарушения функционирования аппаратно-программных ресурсов КВОИ путем планирования и внедрения в процессе его эксплуатации процедур предварительного тестирования вносимых в КВОИ изменений, управления учетными записями, аудита событий информационной безопасности, управления критическими обновлениями, инструментальным контролем информационной защищенности, идентификацией уязвимостей и их устранением.

Мероприятия по разработке и реализации планов реагирования на инциденты безопасности КВОИ направлены на планирование и реализацию процедур регистрации и реагирования на инциденты информационной и физической безопасности КВОИ с распределением ролей и обязанностей, первоочередных действий, правил ведения записей.

Мероприятия по разработке и реализации планов восстановления КВОИ после инцидентов безопасности направлены на планирование и реализацию процедур восстановления устойчивого функционирования КВОИ, а также периодический пересмотр их эффективности с дальнейшими корректирующими действиями по всем мероприятиям, направленным на обеспечение защищенности КВОИ.

Мероприятия по обеспечению надежного функционирования КВОИ в процессе эксплуатации направлены на снижение рисков нарушения штатного функционирования КВОИ в результате выхода из строя его ресурсов путем резервирования его компонентов, использования конструктивных решений, обеспечивающих повышенную надежность, своевременного проведения работ по обслуживанию и реагированию на сбои в ресурсах.

Мероприятия по техническому обследованию КВОИ для оценки соответствия состояния ТЗИ установленным требованиям направлены на обеспечение независимого контроля состояния безопасного штатного функционирования КВОИ путем оценки полноты и качества реализованных мер с учетом условий и особенностей функционирования КВОИ.

**5.5** Все мероприятия по обеспечению защиты КВОИ должны координироваться и дополнять друг друга, создавая состояние его защищенности с учетом актуальных угроз. Нарушение любого из требований, реализующих мероприятие по безопасности, может быть основанием для его пересмотра и принятия дополнительных требований по этому и другим мероприятиям.

**5.6** Владелец КВОИ КИ обязан обеспечить его безопасное функционирование. В случае непринятия (принятия недостаточных) мер по обеспечению безопасного функционирования КВОИ владелец несет ответственность в соответствии с действующим законодательством Республики Беларусь.

**5.7** Безопасность КВОИ КИ должна рассматриваться как важнейший компонент политики безопасности, представляющей собой совокупность документированных правил, процедур и требований в области защиты информации, действующих в организации [4].

## **6 Распределение обязанностей по обеспечению безопасности критически важных объектов информатизации**

### **6.1 Назначение ответственного лица**

**6.1.1** Руководитель объекта КИ должен назначить ОДЛ из состава руководства.

ОДЛ должно обладать глубокими знаниями целей и задач функционирования объекта отраслевой инфраструктуры, знаниями в области информационных технологий и информационной безопасности, экологической безопасности (для автоматизированных систем управления технологическими процессами), проектирования систем безопасности, уметь объединять людей, компетентных в различных областях знаний, в эффективно работающую группу.

В обязанности ОДЛ входит выполнение следующих основных функций:

– советника руководителя объекта КИ по вопросам информационной безопасности;

- руководство специалистами по информационной безопасности, реализацией системы защиты КВОИ, контроль за разработкой документации по информационной безопасности (политика безопасности, задание по безопасности, инструкции, процедуры, руководства и т.д.);

- проведение оценки риска нарушения информационной безопасности КВОИ, подготовка предложений по внедрению мер повышения информационной безопасности КВОИ;

- планирование и координация обучения персонала в области информационной безопасности;

- руководство действиями во время инцидентов, исследование инцидентов, связанных с нарушением информационной безопасности, периодическая проверка реализованных мер информационной безопасности КВОИ и др.

Для решения проблем информационной безопасности должна быть создана группа информационной безопасности, работающая под руководством ОДЛ. Группа должна соответствовать следующим требованиям:

- а) состоять из специалистов, постоянно работающих на объекте, экспертов в области информационных технологий и специалистов по компьютерным системам для конкретных устройств объекта инфраструктуры. Специалисты должны быть сертифицированы на профессиональную компетентность в области защиты информации;

- б) быть обеспеченной необходимыми ресурсами;

- в) иметь четкое разграничение ответственности между специалистами группы и координацию деятельности;

- г) регулярно собираться для решения следующих задач:

- выполнять анализ риска;

- определять и реализовывать меры противодействия угрозам;

- сопровождать план обеспечения информационной безопасности и всю документацию по информационной безопасности;

- определять общие цели и стратегии информационной безопасности;

- обеспечивать надзор за структурой вычислений системы;

- оценивать эффективность мер информационной безопасности;

- обеспечивать тренинги обучение персонала в области информационной безопасности;

- анализировать и исследовать инциденты информационной безопасности.

**6.1.2** Руководители подразделений, обслуживающих КВОИ, несут ответственность за обеспечение соответствующего уровня его безопасности в пределах их служебных обязанностей и обеспечивают выполнение следующих задач:

- планирование, реализацию, тестирование и эксплуатацию КВОИ с учетом всех правил политики информационной безопасности;

- периодическое усовершенствование реализованных мер в соответствии с изменениями в угрозах или уязвимости;

- периодический контроль качества продукции и услуг внешних поставщиков;

- повышение уровня знаний и понимания проблемы информационной безопасности штатом подразделения;

- координацию мер с ОДЛ и другими заинтересованными отделами.

## **6.2 Организация работы с персоналом**

**6.2.1** Персонал КВОИ должен быть осведомлен в безопасности, иметь высокий уровень профессиональной компетентности, профессиональной подготовки, подтвержденный соответствующими документами.

**6.2.2** Организация работы с персоналом КВОИ должна включать:

- повышение осведомленности: программа осведомленности персонала КВОИ в безопасности должна быть разработана, документально оформлена, иметь юридическую силу и поддерживаться для гарантии, что персонал выполняет требования ТНПА, получая непрерывную поддержку обоснованным действиям по безопасности;

– тренинги: весь персонал, получающий доступ к КВОИ, должен быть подготовлен в области правил, средств контроля доступа, процедур управления доступом, их применения, использования важной информации, касающихся КВОИ и критичных ресурсов объекта инфраструктуры;

– отчетность: должны подготавливаться и вестись отчеты для документального оформления обучения, повышения осведомленности и проверки всего персонала, имеющего доступ к КВОИ и критичным активам объекта инфраструктуры.

При приеме на работу должна быть предусмотрена проверка благонадежности специалистов в соответствии с законодательством.

**6.2.3** Для реализации требований по организации работы с персоналом должны быть реализованы следующие мероприятия:

а) повышение осведомленности: разработка и поддержка программы осведомленности персонала через поддержку и продвижение надежных инструкций по безопасности, реализующих требования ТНПА, включая повышение осведомленности о безопасности, используя, по крайней мере, ежеквартально, один или несколько из следующих механизмов:

– непосредственные сообщения (например, по электронной почте, мультимедиа, обучение на базе СВТ и др.);

– памятки по безопасности (плакаты, электронные документы, рассылаемые по компьютерной сети предприятия, брошюры и т.д.);

– поддержку руководством организационных вопросов информационной безопасности (презентации, собрания рабочего коллектива и др.);

б) повышение квалификации: разработка и поддержка программы специального обучения в области информационной безопасности, которая включает, как минимум, следующие обязательные вопросы:

– политику информационной безопасности;

– контроль физического и электронного доступа к критичным компьютерным ресурсам;

– специфику передачи информации о критичных ресурсах ОИ;

– планы действий и процедуры по восстановлению или переустановке критичных ресурсов ОИ и доступа к ним после инцидента безопасности;

в) ведение учетных записей: подготовка и хранение записи для адекватного документального оформления соответствия персонала установленным требованиям, в том числе:

– документацию обо всем персонале, имеющем доступ к ресурсам КВОИ и датах завершения их обучения;

– документацию о том, что программа обучения ежегодно пересматривается;

г) проверка биографических данных:

– ведение списка всего персонала, имеющего доступ к ресурсам КВОИ, включая их индивидуальные права на электронный и физический доступ к критичным ресурсам КВОИ внутри периметра (периметров) безопасности;

– ежеквартальный просмотр документов, относящихся к персоналу, и обновление распечаток в течение двух рабочих дней при любом существенном изменении персонала;

– аннулирование доступа в течение 24 ч для любого лица, изменение в статусе которого запрещает ему доступ к критичным ресурсам ОИ (например, истечение срока, временное прекращение работы, перевод на другое место, запрос доступа с сопровождением, и др.);

– осуществление проверки всего персонала до предоставления доступа к критичным ресурсам КВОИ в соответствии с законодательством и подчинение существующему коллективному соглашению индивидуальных договоров.

– новая проверка должна проводиться, по крайней мере, каждые пять лет или по какой-либо причине.

### **6.3 Организация обслуживания в процессе эксплуатации**

**6.3.1** Владельцу КВОИ необходимо строго подходить к выбору поставщика СВТ и сервисной организации по их обслуживанию:

**6.3.2** Для обеспечения безопасного взаимодействия при обслуживании и поставках систем на основе СВТ и их компонентов необходимо выполнение следующих требований:

- служба информационной безопасности КВОИ должна работать в тесном сотрудничестве с подразделением по контрактам для гарантии, что условия информационной безопасности учтены в любом контракте;
- контракты, определяющие порядок защиты критичной информации и активов компаниями-контрагентами на их собственной территории, имеют статус критичности, установленный владельцем;
- маркированная по уровням критичности информация и относящиеся к ней активы должны рассматриваться как подверженные риску компрометации или несанкционированного раскрытия;
- для гарантии того, что основные мероприятия по информационной безопасности выполняются, должно с самого начала обеспечиваться и контролироваться на протяжении всего времени заключения и выполнения контракта рабочее взаимодействие ответственных подразделений с организацией-подрядчиком.

**6.3.3** Служба информационной безопасности КВОИ должна проводить проверки компании-подрядчика, чтобы убедиться, что выполняются следующие требования:

- в качестве руководителя службы информационной безопасности (инспектора) назначен служащий соответствующего статуса и компетентности;
- член руководства предприятия-подрядчика официально принял на себя полную ответственность за информационную безопасность;
- служащие, которые должны иметь доступ к критичной информации, проверены на благонадежность и им присвоены соответствующие полномочия;
- подрядчик имеет в наличии соответствующий ТНПА, охватывающий области физической, информационной безопасности и безопасности персонала;
- имеются внутренние документированные процедуры по информационной безопасности, доступные всем, кто будет отвечать за информационную безопасность или имеет доступ к активам, охраняемым в соответствии с категорией информации;
- персонал проинструктирован о своих обязанностях;
- для защиты категорированной информации, относящейся к контракту, подрядчик использует принцип "необходимо знать";
- соответствующие ТНПА информационной безопасности сопровождаются и периодически анализируются на протяжении контракта;
- установлены соответствующие ограничения на использование информационных систем для обработки и передачи защищаемой категорированной информации и данных;
- руководитель службы информационной безопасности подрядчика письменно подтверждает перед руководством КВОИ (организацией-заказчиком), что служащие его компании, имеющие отношение к контракту, получили соответствующие уровни допуска.

**6.3.4** Текущая проверка и требования благонадежности для доступа к защищаемой маркированной информации могут быть организованы следующим образом:

- после подписания контракта подрядчику должен быть направлен бумажный документ, определяющий те элементы контракта, которые требуют категорирования информации по уровню критичности и соответствующей маркировки, которая будет применена к отдельным областям контракта. Формат этого документа должен соответствовать требованиям действующего законодательства Республики Беларусь. Он может составлять часть контракта или разрабатываться отдельно;
- по всем контрактам заключившее их руководство несет ответственность, гарантируя, что условия контрактов будут соблюдаться;
- руководитель службы безопасности КВОИ должен планировать периодические оценки соблюдения согласованных требований безопасности для гарантии, что они доведены до сведения на местах и удовлетворительно выполняются.

## **7 Обеспечение информационной безопасности**

**7.1** Для обеспечения информационной безопасности КВОИ в процессе эксплуатации необходимо:

- определить цели безопасности КВОИ;
- распределить ответственность по всем аспектам информационной безопасности, которые интегрируют безопасность КВОИ в безопасность объекта инфраструктуры;
- разработать задание по безопасности на КВОИ;
- предусмотреть соответствующие ресурсы на защиту КВОИ;
- ввести в действие реализуемую политику информационной безопасности, одобренную высшим руководством, реализовать требования задания по безопасности;
- обеспечить периодическое обновление политики информационной безопасности и процедур;
- обеспечить обновление задания по безопасности при изменении технологии обработки информации либо изменении рисков;
- обеспечить согласованность политики информационной безопасности и процедур, задания по безопасности с законодательством и руководствами.

**7.2** Для выявления уязвимостей (слабых мест), которые на стадии проектирования КВОИ могли быть допущены как следствие различных подходов к реализации конкретных технических требований, должна быть критически проанализирована и упорядочена вся доступная информация, источниками которой могут быть:

- спецификация требований, техническое задание на проектирование, технические требования на внедрение, спецификация тестов;
- задание по безопасности;
- данные оперативного контроля, управление сообщениями и изменениями требований;
- описание функциональных свойств (задачи, функции, режимы, связи, структуры), задаваемых в спецификации на КВОИ;
- описание нефункциональных свойств КВОИ, задаваемых в спецификации (доступность, надежность, защита, безопасность, гибкость, удобство сопровождения, частота использования, мобильность и др.).

**7.3** Среда угроз информационной безопасности и соответствующие им сценарии быстро изменяются, поэтому любая система в составе КВОИ должна быть обеспечена системой активной и непрерывной оценки угроз, о которой необходимо регулярно докладывать руководству.

**7.4** Система информационной безопасности КВОИ должна обеспечивать регистрацию всех инцидентов безопасности, обеспечивать возможность их быстрого анализа и принятия решений по совершенствованию действующих и реализации дополнительных мер по повышению качества управления безопасностью КВОИ.

**7.5** Используемые средства обеспечения информационной безопасности КВОИ должны исходить из требований политики информационной безопасности верхнего уровня (объекта инфраструктуры) и политики информационной безопасности собственно КВОИ, задания по безопасности, выполнение которых контролируется в процессе эксплуатации.

**7.6** Требования к организации управления информационной безопасностью КВОИ:

- а) разработать и поддерживать политику информационной безопасности объекта инфраструктуры и обеспечить управление этой политикой;
- б) идентифицировать всю информацию, независимо от видов носителя, относящуюся к КВОИ. Эта информация должна включать доступ к процедурам, список критичных активов, топологии, планы размещения, конфигурации и любую относящуюся к безопасности информацию;
- в) обеспечить категорирование информации, относящейся к КВОИ, чтобы помочь персоналу, имеющему доступ к этой информации, определить, какая информация может быть раскрыта неавторизованному персоналу, а также относительную критичность информации, которая не должна раскрываться вне предприятия без соответствующего разрешения;
- г) установить ограничения на доступ к информации, относящейся к КВОИ, в соответствии с ее категорией:

- назначить представителя из состава высшего руководства с обязанностями по руководству и управлению внедрением на предприятии ТНПА по безопасности. Это лицо должно иметь право на авторизацию любого отклонения или исключения из требований настоящего документа. Любое отклонение или исключение из требований должно быть документально оформлено;

- определить роли и ответственность собственников, владельцев, пользователей, персонала охраны в отношении КВОИ;

- определить роли и ответственность при доступе, использовании и обработке критичной информации;

- определить и документально оформить структуру отношений и процессов принятия решений, которые определяют и демонстрируют способность руководства на уровне исполнительной власти управлять и контролировать предприятие, чтобы обеспечить безопасность КВОИ;

- установить и оформить документально процесс управления доступом к информации, относящейся или используемой КВОИ, компрометация которой может повлиять на надежность и/или доступность системы управления КВОИ, за которую организация несет ответственность;

- д) составить список персонала, который несет ответственность за авторизованный доступ к КВОИ:

- логический и физический доступ к КВОИ может быть разрешен только персоналом, отвечающим за авторизованный доступ к этим активам;

- все разрешения на доступ должны быть оформлены документально;

- анализировать права на доступ к информации КВОИ, чтобы подтвердить, что они правильные, согласуются с потребностями организации и соответствуют ролям и обязанностям;

- определить процедуры для гарантии, что модификация, временная приостановка или прекращение доступа пользователей к КВОИ выполняется в течение 24 ч с момента изменения статуса пользователя доступа. Все аннулирования/изменения должны быть официально разрешены и оформлены документально;

- е) для ввода в эксплуатацию:

- ОДЛ должны определить средства контроля для тестирования и оценки новых или обновляемых систем и программных изменений;

- регулирующие органы должны назначить полномочные организации, которые будут проводить внешний контроль и выдавать официальное заключение о том, что КВОИ соответствует требованиям информационной безопасности;

- полномочные организации несут ответственность по заключению, что КВОИ прошел контроль, соответствует требованиям безопасности и может быть допущен к дальнейшей эксплуатации.

**7.7** Для реализации требований по управлению информационной безопасностью КВОИ должны выполняться следующие мероприятия:

- а) политика информационной безопасности и задание по безопасности:

- обеспечить выполнение разработанной политики информационной безопасности, формулирующую обязанности по защите КВОИ;

- пересматривать политику информационной безопасности по крайней мере ежегодно;

- обеспечить документирование любых отклонений или исключений, официально разрешенных представителем действующего высшего руководства, отвечающим за программу информационной безопасности;

- анализировать все официально разрешенные отклонения и исключения, по крайней мере, ежегодно и оформлять документально пределы распространения или аннулирования любых пересмотренных авторизованных отклонений или исключений;

- обеспечить реализацию требований задания по безопасности в системе защиты;

- пересматривать задание по безопасности в случаях изменения технологии обработки информации либо изменения рисков и инцидентов безопасности;

- б) защита информации:

- анализировать программу обеспечения защиты информации, по крайней мере, ежегодно;

- выполнять оценку программы обеспечения защиты информации для гарантии соответствия с документированным процессом, по крайней мере, ежегодно;

- оформить документально процедуры, используемые для защиты информации, которая была идентифицирована как критически важная информация, согласно уровню критичности, назначенному этой информации;

- установить процедуры идентификации и классификации критичной информации КВОИ для гарантии соответствия документированным процессам, по крайней мере, ежегодно;

в) роли и обязанности:

- назначить ответственное лицо из состава высшего руководства, ответственное за программу информационной безопасности, с указанием имени, должности, телефона, адреса и даты назначения;

- отслеживать установленные роли и обязанности по обработке критичной информации КВОИ в соответствии с политикой информационной безопасности;

- организовать документирование всех изменений в ролях и обязанностях в течение 30 дней со дня вступления их в силу;

- пересматривать роли и обязанности владельцев, охраны и пользователей КВОИ, по крайней мере, ежегодно;

- управление: анализировать структуру внутренних корпоративных отношений и процессов, относящихся к программе информационной безопасности, по крайней мере, ежегодно, для гарантии, что существующие отношения и процессы продолжают, обеспечивая соответствующий уровень подотчетности, и что высшее руководство непрерывно участвует в этом процессе;

г) авторизация доступа:

- обновлять список назначенного персонала, ответственного за авторизованный доступ к критичной электронной информации, в течение пяти дней при любом изменении в статусе, который влияет на возможность назначенного персонала разрешать доступ к критичным активам ОИ;

- список назначенного персонала, ответственного за авторизацию доступа к критичным активам КВОИ должен пересматриваться, как минимум, раз в квартал;

- список назначенного персонала, ответственного за авторизацию доступа к критичным активам КВОИ должен идентифицировать каждое лицо по имени, должности, номеру телефона, адресу, дате назначения и системе/приложению, за авторизацию доступа к которым они несут ответственность;

- анализировать процессы для назначения привилегий на доступ, отсрочки или блокирования учетных записей пользователя. Этот анализ должен быть оформлен документально. Процесс должен периодически переоцениваться, чтобы гарантировать соответствие с правилами, по крайней мере, ежегодно;

- проверять права пользователя на доступ к критичным ресурсам КВОИ ежеквартально, чтобы подтвердить, что доступ еще необходим;

д) разрешение на ввод систем в эксплуатацию:

- определить конкретных лиц по имени, должности, телефону, адресу и дате назначения, ответственных за разрешение на ввод в эксплуатацию КВОИ, пригодных для производственной среды, с правом утверждения этого разрешения;

- изменения в кандидатуре назначенного должностного лица с правом разрешения должно быть документально оформлено в течение 48 ч с изменениями, имеющими силу.

**7.8** С целью оценки уровня информационной безопасности КВОИ до ввода его в эксплуатацию в обязательном порядке проводится аттестация его системы защиты информации на соответствие требованиям НПА, в том числе ТНПА в области защиты информации, задания по безопасности и выдача на этой основе аттестата соответствия.

**7.9** Аттестация включает следующие виды проверок и обязательных мероприятий [4]:

- анализ организационной структуры и информационных потоков объекта КИ, состава и структуры комплекса технических средств и ПО системы защиты информации КВОИ, документации на КВОИ и ее соответствия требованиям НПА и ТНПА в области защиты информации;

- проверку правильности отнесения КВОИ к соответствующему классу по уровню безопасности, назначения требований, выбора и применения соответствующих средств защиты информации;

- анализ результатов испытаний системы и средств защиты информации;

- проверку уровня подготовки кадров и распределения ответственности персонала за организацию и выполнение требований по защите информации;

- оценку системы защиты информации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

- оформление протоколов испытаний (оценки) и заключения по результатам проверок.

**7.10** Результаты аттестации должны отразить:

- текущее состояние организационной структуры объекта, в составе которого функционирует КВОИ;

- риски нарушения безопасности КВОИ в рамках объекта КИ;

- уровень организации управления и мониторинга безопасности КВОИ;

- настройки политики информационной безопасности на серверах и рабочих станциях;

- состояние антивирусной защиты серверов и рабочих станций;

- организацию обмена данными в рамках объекта инфраструктуры;

- организацию хранения данных у владельца КВОИ;

- настройку резервного копирования данных на серверах рабочих станций пользователей;

- организацию функционирования КВОИ (правила и инструкции для работы пользователей, применяемые ТНПА и политики безопасности).

**7.11** Детализированное описание процедур и последовательности проведения аттестации КВОИ должно быть приведено в рабочих программах и методиках аттестации, разрабатываемых до этапа аттестации с учетом назначения и конкретной реализации КВОИ.

## **8 Обеспечение сетевой безопасности**

**8.1** Обеспечение требований безопасности деловых и технологических процессов, поддерживаемых с использованием КВОИ, взаимодействующим с другими системами для предоставления данных, приводят к повышенному риску компрометации или разрушения его ресурсов.

Для защиты ресурсов КВОИ при его взаимодействии с другими системами необходимо идентифицировать электронный периметр безопасности КВОИ, в пределах которого он находится.

Электронный периметр безопасности КВОИ является логической границей, окружающей сеть или группу подсетей ("защищенная сеть"), в которой функционирует КВОИ, логический доступ к которой контролируется.

**8.2** После того, как электронный периметр КВОИ определен, ему может быть назначен соответствующий уровень безопасности в зависимости от класса КВОИ в пределах этого электронного периметра и требований к организации его защиты.

**8.3** Требования к организации защиты электронного периметра безопасности КВОИ включают:

а) определение электронного периметра безопасности:

- идентифицировать электронный периметр безопасности КВОИ и все точки доступа к периметру;

- точки доступа к электронному периметру должны дополнительно включать любую подключенную извне конечную точку связи (например, модемы), оканчивающуюся на устройстве внутри электронного периметра;

– линии коммуникаций, связывающие отдельные электронные периметры не рассматриваются как часть периметра электронного безопасности. Однако конечные точки этих линий коммуникаций внутри периметров безопасности рассматриваются как точки доступа к электронным периметрам;

б) контроль электронного доступа:

– обеспечить организационные, технические процессы и процедуры для контроля логического доступа на всех точках электронного доступа к электронному периметру и КВОИ внутри него;

– средства контроля должны реализовать модель контроля доступа, которая отказывает в доступе по умолчанию до тех пор, пока не определено установленное разрешение;

– там, где реализован внешний интерактивный логический доступ к точкам электронного доступа в электронный периметр безопасности, необходимо реализовать сильные процедурные или технические меры для гарантии аутентификации субъекта, осуществляющего доступ;

– устройства электронного контроля доступа должны предоставить пользователю соответствующее сообщение о попытках интерактивного доступа;

– мониторинг управления доступом: реализовать организационные, технические и методические средства контроля доступа, включая инструментарий и процедуры для мониторинга авторизованного доступа, определения неавторизованного доступа (вторжения) и попыток неавторизованного доступа к электронному периметру и критичным активам КВОИ в режиме "24 часа 7 дней в неделю";

в) анализ документов и сопровождение:

– обеспечить гарантии, что вся документации отражает текущую конфигурацию и процессы КВОИ;

– проводить периодические ревизии этих документов для гарантии их правильности и своевременно обновлять все документы вслед за введением изменений.

**8.4** Мероприятия по реализации требований к защите электронного периметра безопасности КВОИ включают:

а) электронный периметр безопасности:

– необходимо вести документацию или набор документов, описывающих электронный периметр безопасности КВОИ, все взаимосвязанные КВОИ внутри электронного периметра безопасности, все точки электронного доступа в периметр безопасности и взаимосвязанные среды;

– документ или набор документов должен удостоверить, что все КВОИ находятся внутри электронного периметра безопасности;

б) контроль электронного (логического) доступа:

– вести документацию или набор документов, описывающих организационные, технические и процедурные средства контроля электронного (логического) доступа и их реализацию для каждой точки электронного доступа к электронному периметру;

в) для каждого средства контроля документ или набор документов должны идентифицировать и описать, как минимум:

– запрос на доступ и процесс авторизации;

– реализованные для этого средства контроля;

– используемый метод аутентификации и процесс периодического анализа авторизованных прав в соответствии с установленной политикой управления и контроля;

– действующую сопроводительную документацию (например, запрос доступа и документы по авторизации, анализ списка контроля доступа), удостоверяющую, что эти меры были реализованы;

г) мониторинг управления электронным доступом:

– вести документацию мониторинга электронного (логического) доступа, устанавливающую организационные, технические и процессуальные средства контроля, включая инструментарий и процедуры;

– документация должна определять вспомогательные документы, включающие записи и регистрацию доступа, чтобы подтвердить, что инструментарий и процедуры функционируют и используются в соответствии с проектом;

– дополнительные документы или набор документов должны установить и описать процессы, процедуры, технические средства контроля и сопровождающие их документы, реализованные для подтверждения регистрации авторизованного доступа в соответствии правами контроля доступа, доклады и тревожные сообщения о неавторизованном доступе и попытках неавторизованного доступа для соответствующего персонала, осуществляющего мониторинг;

д) анализ документации и сопровождение: просматривать и обновлять документы, относящиеся к вышеприведенным разделам, по крайней мере, ежегодно или в пределах 90 дней с момента модификации сети или средств контроля.

## **9 Обеспечение физической безопасности**

**9.1** Система обеспечения физической безопасности КВОИ должна противостоять угрозам, связанным с непосредственным физическим доступом к его компонентам и возможным диверсиям, предотвращать или минимизировать их последствия и обеспечивать:

- обнаружение попыток и защиту от проникновения нарушителя на территорию КВОИ и оповещение караульной службы о нарушении;
- видео наблюдение за территорией КВОИ;
- контроль и управление доступом на территорию КВОИ и к ресурсам КВОИ;
- сбор, обработку и хранение информации, полученной в процессе наблюдения;
- телефонную связь;
- освещение территории;
- резервное электропитание.

**9.2** При разработке системы физической защиты КВОИ должен использоваться принцип многоуровневой защиты (принцип "защиты в глубину").

**9.3** Требования по обеспечению физической безопасности КВОИ включают:

- а) периметр физической безопасности:
  - определить физический периметр безопасности, внутри которого размещается КВОИ, все точки доступа к этому периметру и разработать стратегию "защиты в глубину" для физической защиты КВОИ;
  - присвоить физическому периметру безопасности КВОИ уровень обеспечиваемой безопасности в зависимости от класса КВОИ;
- б) контроль физического доступа:
  - реализовать необходимые меры по контролю доступа ко всем точкам доступа периметра и критичным активам внутри него: доступные точки физического периметра безопасности должны включать все точки физического входа или выхода через ближайшую физически защищенную четырьмя стенами границу, окружающую КВОИ;
  - внедрить организационные, технические и процедурные средства управления физическим доступом ко всем доступным точкам физического периметра безопасности;
- в) мониторинг физического доступа: реализовать организационные, технические и процедурные средства, включая инструментальный и процедуры, для мониторинга физического доступа в режиме "24 часа 7 дней в неделю";
- г) регистрация физического доступа: внедрить технические и процедурные механизмы для регистрации физического доступа;
- д) сопровождение и тестирование: реализовать всестороннее сопровождение и тестирование программ для гарантии, что все физические системы защиты (например, контакты на дверях, детекторы движения, замкнутая система телевизионного наблюдения и др.) действуют на границе периметра, определяя неавторизованные действия;
- е) документирование: оформлять документально реализацию всех требований по обеспечению физической безопасности КВОИ.

**9.4** Для реализации требований по обеспечению физической безопасности КВОИ должны выполняться следующие мероприятия:

- а) анализ документации и сопровождение плана: пересматривать и обновлять действующий план физической безопасности, по крайней мере, ежегодно или в течение 90 дней после модификации изменений в периметре или методах физической защиты;

б) периметр физической безопасности: поддерживать документ или совокупность документов, описывающих периметры физической безопасности и все точки доступа к каждому периметру. Документ должен удостоверить, что все КВОИ размещены внутри физического периметра безопасности;

в) контроль физического доступа:

– реализовать один или несколько методов контроля физического доступа;

– поддерживать документацию, идентифицирующую средства контроля доступа, реализованные для каждой точки физического доступа через физический периметр безопасности;

– документация должна идентифицировать и описывать, как минимум, запрос на доступ, процесс авторизации и отмены авторизации, реализованный для этого вида контроля, и процесс периодического анализа прав авторизации в соответствии с правилами управления, установленными средствами контроля и текущей документацией по их сопровождению;

г) мониторинг физического доступа:

1) реализовать один или несколько из следующих методов:

– видеонаблюдение, которое фиксирует и делает запись изображения действий внутри и вокруг периметра безопасности (замкнутая система телевизионного наблюдения);

– тревожную сигнализацию на основе состояния контакта, показывающего, были ли закрыты дверь или ворота. Эти тревожные сигналы должны идти на центральную станцию мониторинга безопасности или диспетчеру объекта инфраструктуры (примеры – контакты на окнах, дверях, датчики движения);

2) дополнительно поддерживать документацию, описывающую методы мониторинга физического доступа. Эта документация должна определять процедуры сопровождения для проверки, что инструментарий и процедуры мониторинга функционируют и используются в соответствии с проектом. Документация должна идентифицировать и описывать процессы, процедуры и средства эксплуатационного контроля для проверки регистрации доступа на соответствие правам управления доступом;

3) поддерживать процесс создания отчетов о неавторизованных случаях доступа;

д) регистрация физического доступа:

1) запись входа в журнале регистрации должна содержать информацию для идентификации каждого индивидуума, для чего необходимо реализовать один или несколько из следующих методов регистрации:

– ручная регистрация: книга регистрации или ведомость физического доступа, сопровождаемая визуальным контролем человека;

– автоматизированная регистрация: электронная регистрация, выполняемая отобранными средствами контроля и методами мониторинга;

– видеозапись: электронная фиксация видеоизображений;

2) дополнительно к этому необходимо поддерживать документацию, описывающую методы регистрации физического доступа. Эта документация должна определять процедуры поддержки для подтверждения того, что инструментарий и процедуры регистрации функционируют и используются в соответствии с проектом;

3) журналы регистрации физического доступа должны сохраняться, как минимум, 90 дней;

е) сопровождение и тестирование систем физической безопасности: необходимо хранить документацию о ежегодном обслуживании и тестировании систем физической безопасности на протяжении одного года.

## **10 Управление безопасной эксплуатацией**

**10.1** Для управления безопасной эксплуатацией КВОИ необходимо разработать программу, которая направлена на минимизацию или предотвращение риска разрушения или компрометации ресурсов КВОИ при неправильном использовании или компьютерной атаке.

**10.2** Требования к организации управления безопасной эксплуатацией КВОИ включают:

а) процедуры тестирования:

- все новые системы и существенные изменения в действующих КВОИ должны использовать документированные процедуры тестирования на информационную безопасность, дополняющие процедуры функционального тестирования и приемки. Тесты необходимы для предотвращения риска от известных уязвимостей, влияющих на действующие системы, приложения или сетевые сервисы;

- процедуры тестирования на безопасность должны требовать, чтобы тестирование и приемка проводились в контролируемой непроизводственной среде;

- все тестирование должно выполняться способом, который предотвращает отрицательное воздействие на производственную систему и операции;

б) управление паролями и учетными записями:

- разработать руководство по обеспечению аутентификации пользователей для доступа, возможности аудита действий пользователей, минимизации риска неавторизованного доступа к системе при компрометации паролей пользователей;

- разработать порядок управления паролями пользователей, реализуемый и оформленный документально, который включает:

- при отсутствии более совершенных методов, например многофакторного управления доступом, учетные записи должны иметь сложные пароли. Например, пароль, состоящий из комбинации букв, цифр и специальных символов до расширения, допускаемого средой эксплуатации;

- пароли должны периодически заменяться с учетом риска, основанного на частоте угроз, для уменьшения риска взлома пароля;

в) управление исходными учетными записями:

- разработать процесс для управления по умолчанию учетными записями, например, администратора или гостя. Процесс должен включать по возможности удаление и переименование этих учетных записей;

- для учетных записей, которые должны сохраняться, пароли должны быть заменены до ввода системы в обслуживание;

- при наличии технической возможности должны использоваться индивидуальные учетные записи (в противоположность учетным записям группы);

- там, где индивидуальные учетные записи не поддерживаются, ответственное лицо должно иметь правило управления соответствующим использованием учетных записей групп, которое ограничивает доступ только теми, кто авторизован, запись аудита об использовании учетной записи и действия по защите учетных записей в случае перемен в штате, например, изменения должности или уход;

г) анализ доступа:

- анализировать доступ к КВОИ, например, учетные записи, касающиеся доступа к СВТ и/или сети, а также изменения, связанные с назначением или изменением прав доступа, по крайней мере, раз в полгода;

- неавторизованные, недействительные, утратившие силу по истечении срока или неиспользуемые учетные записи доступа к СВТ и/или сети должны быть заблокированы;

д) допустимое использование привилегий: установить правило, применяемое для управления областью и допустимым использованием привилегий администратора и учетных записей других групп. Правило должно обеспечивать аудит использования всех учетных записей до отдельно поименованного лица, например, отдельно поименованные учетные записи пользователя или персональная регистрация для некоторых учетных записей групп, чтобы установить подотчетность использования;

е) управление критичными обновлениями:

- установить формальный порядок управления критичными обновлениями для отслеживания, тестирования и своевременной инсталляции применимых заплат безопасности и обновлений для КВОИ;

- для документирования их внедрения или причины отказа от инсталляции использовать процессы формального контроля и управления конфигурацией;

- в случае невозможности инсталляции заплаты принять и оформить документально компенсирующую меру;

ж) целостность ПО: использовать формально документируемый процесс управления применением антивирусных и других инструментальных средств обеспечения целостности систем для предупреждения, ограничения подверженности и/или предотвращения внесения через электронную почту, браузеры и интернет вредоносных программ в активы до и внутри электронного периметра безопасности;

и) идентификация уязвимостей и ответные действия:

– как минимум ежегодно, проводить оценку уязвимостей, включающую диагностический анализ (контролируемое тестирование на проникновение) точек доступа к электронному периметру безопасности, сканирование открытых портов/сервисов и модемов, учетных записей по умолчанию, заплат безопасности и уровней антивирусных версий;

– выполнять документально оформленный план действий по управлению, чтобы исправить уязвимости и недостатки, если они идентифицированы при оценке;

к) сохранение системных записей регистрации:

– все КВОИ должны генерировать запись аудита для всех событий системы, относящихся к безопасности, обеспечить сохранность данных регистрации на период в 90 дней;

– в случае, если инцидент сетевой безопасности обнаруживается в пределах периода хранения до 90 дней, регистрационные записи должны храниться на протяжении трех лет в экспортируемом формате для возможного использования при анализе дальнейших событий;

л) контроль изменений и управление конфигурацией:

– организовать процесс управления изменениями, который предусматривает контролируемую среду модификации всех аппаратных и программных средств КВОИ;

– процесс должен включать процедуры управления изменениями, который, как минимум, обеспечивает тестирование, запись аудита модификации, проблемы идентификации, процессы возврата и восстановления, разрушение модификаций и, в конечном счете, гарантировать общую целостность КВОИ;

м) блокировать отдельные неиспользуемые порты/сервисы;

н) обеспечить безопасность связанного оборудования;

п) эксплуатационное состояние инструментальных средств: компьютерные и коммуникационные системы, используемые для управления КИ в составе КВОИ, должны, как минимум, включать или дополняться автоматическими инструментальными средствами для контроля эксплуатационного состояния, коэффициента использования и эффективности процессов;

р) резервное копирование:

– резидентная информация на КВОИ, используемая для управления КИ, должна регулярно копироваться, а копия передаваться на удаленное средство обслуживания;

– архивная информация, сохраняемая на машинном носителе в течение длительного времени, должна тестироваться, по крайней мере, ежегодно для гарантии, что эта информация воспроизводима.

**10.3** Для реализации требований по обеспечению безопасной эксплуатации КВОИ должны выполняться следующие мероприятия:

а) процедуры тестирования:

– для всех КВОИ документация ответственного лица по контролю изменений должна включать соответствующие записи о процедурах тестирования, результатах и успешном завершении;

– процедуры тестирования должны также включать все подробности используемой среды, в которой проводилось тестирование;

– документация должна подтвердить, что все изменения в КВОИ были успешно протестированы относительно возможных уязвимостей безопасности до ввода в эксплуатацию на контролируемой вспомогательной системе;

б) управление учетными записями и паролями:

– поддерживать документированную политику паролей и протоколов ежеквартального аудита этой политики по всем учетным записям на КВОИ. Эта документация должна подтвердить, что все учетные записи соответствуют политике паролей и что устаревшие учетные записи заблокированы;

– при обычном административном перемещении персонала организации руководство должно пересматривать разрешение на доступ в течение 5 рабочих дней;

- при вынужденном прекращении работы специалиста руководство должно пересматривать разрешение на доступ в течении не более 24 ч;
- в) управление критичными обновлениями:
  - документация по изменениям в контроле должна включать записи всех инсталляций заплат безопасности, включая дату тестирования, результаты тестирования, разрешение руководства на инсталляцию и дату инсталляции;
  - лицо, ответственно за инвентаризацию КВОИ, должно также включать записи о ежемесячном анализе всех доступных поставляемых заплат/обновлений ОС для безопасности, и текущих уровней анализа/заплат;
  - документация должна удостоверить, что все КВОИ за счет обновления ОС, заплат безопасности и других компенсирующих мер, рассматриваются как имеющие минимальный риск компрометации от известных уязвимостей;
- г) целостность ПО:
  - документация ответственного лица за инвентаризацию КВОИ и изменения контроля, должна включать записи обо всех антивирусах и другом применяемом инструментарии для целостности систем и уровень текущей используемой версии;
  - ведомость инвентаризации КВОИ должна включать записи ежемесячного анализа всех доступных обновлений ПО этих заплат/обновлений ОС и их текущие версии.
  - документация должна подтверждать, что все КВОИ улучшаются на доступном для обеспечения целостности ПО таким образом, чтобы минимизировать риск от инфицирования через электронную почту, браузер или другое вредоносное ПО, порождаемое Интернет;
  - если целостность ПО не обеспечивается для отдельной компьютерной платформы или другой меры компенсации, которая принята для минимизации риска КВОИ, компрометация из-за вирусов или вредоносного ПО должна документироваться;
- д) идентификация уязвимостей и реагирование:
  - поддерживать документацию, идентифицирующую организационные, технические и процессуальные средства контроля, включая инструментарий и процедуры для мониторинга уязвимостей КВОИ;
  - документация должна также включать записи ежегодной оценки уязвимостей и планы исправления всех уязвимостей и/или недостатки, которые были обнаружены;
  - документация должна подтвердить, что ответственное лицо приняло соответствующие меры, направленные на потенциальные уязвимости;
- е) хранение регистрационных записей:
  - поддерживать документацию, которая индексирует местоположение, содержание и режим хранения всех данных регистрации КВОИ;
  - документация должна подтверждать, что ответственное лицо сохраняет информацию, которая может быть жизненно важной для внутренних и внешних расследований инцидентов безопасности, включая КВОИ;
- ж) управление заменой средств контроля и изменениями конфигурации:
  - поддерживать документацию, идентифицирующую средства контроля, включая инструментальные средства и процедуры, для управления изменениями и тестирования КВОИ;
  - документация должна удостоверить, что ответственное лицо соблюдает методический подход к управлению изменениями на КВОИ;
- и) блокирование неиспользуемых сетевых сервисов/портов:
  - документировать состояние/конфигурацию сетевых сервисов и портов КВОИ и записи регулярного аудита всех сетевых сервисов и портов на соответствие политике безопасности и документированной конфигурации;
  - документация должна удостоверить, что ответственно лицо приняло соответствующие меры в точках защищенного электронного доступа к КВОИ;
- к) соединение через связанные устройства:
  - поддерживать документированное правило по безопасности подключений через связанные устройства (модемы) к КВОИ, поддерживать регулярный аудит подключений с указанием портов на соответствие политике и документированной конфигурации.
  - документация должна удостоверить, что ответственное лицо приняло соответствующие меры для безопасного коммутируемого доступа к КВОИ;

л) инструментальные средства для мониторинга эксплуатационного состояния: поддерживать документацию, идентифицирующую организационные, технические и процессуальные средства контроля, включающие инструментарий и процедуры для контроля эксплуатационного состояния, использования и эффективности КВОИ;

м) резервное копирование и восстановление:

– поддерживать документацию, которая индексирует местоположение, содержание и каталоги хранения всех резервных копий и лент;

– документация должна включать процедуры восстановления при реконструкции любого ресурса КВОИ по данным резервной копии и записи ежегодного исследования по проверке восстановления;

– документация должна удостоверяет, что ответственное лицо способно восстановить КВОИ после отказа или компрометации.

## **11 Планирование обеспечения безопасности**

**11.1** Планы обеспечения безопасности КВОИ должны разрабатываться и реализовываться в рамках общего плана защиты объекта КИ, включать сценарии атак на ресурсы КВОИ и предполагать возможность координации физической и кибернетической атак.

**11.2** План информационной безопасности и план физической безопасности КВОИ должны взаимно дополнять друг друга. Оба плана должны разрабатываться с учетом того, что КВОИ могут реализовывать также требования управления физическим доступом, поэтому компрометация их активов может привести к снижению или потере определенных активов физической защиты.

**11.3** План физической безопасности КВОИ и управляемого им специального оборудования должен учитывать возможность диверсий и злоумышленных актов и разрабатываться в условиях закрытых консультаций со специалистами по физической защите, технологическим процессам, сетевой безопасности и информационным технологиям.

**11.4** Планы безопасности КВОИ должны регулярно анализироваться и обновляться, отражая инциденты безопасности и опыт эксплуатации систем безопасности.

**11.5** Планы безопасности КВОИ должны содержать, как минимум, следующие разделы:

а) организация и обязанности: схема организации, ответственность лиц, процесс периодического анализа безопасности и подтверждения его уровня;

б) управление активами:

– схема сети, включающая все подключения к внешним компьютерным системам;

– перечень всех компьютерных систем;

– перечень всех приложений компьютерных систем;

в) управление персоналом:

– обучение;

– требования к квалификации;

– учет перемещений (увольнения);

г) риск, уязвимость и оценка соответствия техническим условиям:

– анализ плана безопасности и периодичность переоценки;

– самооценка (процедуры тестирования на проникновение);

– процедуры аудита и отслеживания уязвимости;

– соответствие требованиям нормативных актов;

д) управление проектированием системы безопасности и конфигурацией: контракт на поставку средств защиты для систем информационной и физической безопасности КВОИ;

е) рабочие процедуры безопасности:

1) контроль доступа:

– категорирование активов;

– аутентификация;

– управление паролями; уровень доступа;

– контроль физического доступа;

– процедура контроля доступа третьей стороны/ поставщика;

2) безопасность данных:

- антивирусное ПО;
- шифрование;
- специальные требования для приложений (например, для электронной почты);
- 3) безопасность коммуникаций:
  - связь по проводной сети;
  - беспроводная связь;
  - безопасные средства сопряжения домена;
  - удаленный доступ;
  - доступ внешней/третьей стороны;
- 4) безопасность платформ и приложений (например, аппаратная реализация);
- 5) мониторинг безопасности компьютерных систем:
  - распознавание вторжения/определение аномалий;
  - регистрация;
- 6) техническое обслуживание компьютерных систем:
  - управление заплатами;
  - установка нового ПО/аппаратных средств;
- ж) обработка инцидентов:
  - 1) идентификация;
  - 2) блокирование;
  - 3) восстановление и реконструкция;
  - 4) составление отчета;
- и) резервирование (дублирование) компьютерных систем.

**11.6** При организации защиты процессов КВОИ локальные планы информационной безопасности должны учитывать все аспекты ежедневно выполняемых операций на местах.

Процесс планирования обеспечения информационной безопасности должен включать следующие основные компоненты:

- поддержку программных и аппаратных средств;
- модификацию управления (замена средств контроля);
- модернизацию ПО в динамически изменяющейся среде (управление заплатами, обновление антивирусных программ и т.д.);
- контроль соответствия принятых мер политикам и планам безопасности, заданию по безопасности;
- мониторинг операций и действий аудитора;
- обработку и исследование инцидентов.

**11.7** Основой планов безопасности КВОИ должна быть четкая программа обучения и тренировок персонала и подрядчиков процедурам безопасности.

**11.8** План информационной безопасности КВОИ должен учитывать дополнительные проблемы, касающиеся систем связи для осуществления бизнес-процессов и сопоставимой по безопасности системы управления процессами за пределами КВОИ.

**11.9** План информационной безопасности КВОИ и относящегося к нему оборудования должен разрабатываться с учетом взаимодействия его компьютерных систем между собой и возможности влияния этого взаимодействия на безопасность КВОИ в неявном виде.

Необходимо провести полную инвентаризацию всех компьютерных систем КВОИ и их взаимодействий. Эти требования отражаются в плане обеспечения безопасности компьютерных систем КВОИ в соответствии со следующей методологией:

- собирается вся информация о компьютерных системах КВОИ для создания общего списка активов;
- взаимодействие между идентифицированными активами отражается в топологической схеме КВОИ;
- описывается и оценивается соотношение функций защиты идентифицированных систем безопасности, систем, относящихся к безопасности, и систем охраны.

**11.10** Для гарантии непрерывности процессов КВОИ в случае непредвиденных событий необходимо разработать стратегии резервирования (дублирования), планы действий на инциденты (нештатные ситуации) и планы восстановления.

**11.11** Меры безопасности, запланированные и реализованные для защиты КВОИ от вторжения, разрушения или иной формы компрометации, должны контролироваться в процессе его эксплуатации непрерывно.

## 12 Разработка и реализация планов реагирования на инциденты

**12.1** План реагирования на инциденты должен быть разработан, оформлен документально и утвержден руководством объекта КИ.

**12.2** План реагирования на инциденты определяет процедуры, которым необходимо следовать, когда установлены инциденты физической или информационной безопасности.

**12.3** План реагирования на инциденты должен предусматривать и обеспечивать при реализации возможность сообщения и реагирования на инциденты, связанные с физической и информационной безопасностью, для исключения и/или минимизации их воздействия на КВОИ и объект КИ в целом.

**12.4** План реагирования на инциденты должен содержать следующие разделы:

а) классификацию инцидентов безопасности КВОИ: необходимо определить процедуры, характеризующие и классифицирующие события, связанные с нарушением безопасности, как инциденты физической и информационной безопасности КВОИ;

б) сообщения об инцидентах безопасности КВОИ: необходимо докладывать об инцидентах обычных и инцидентах информационной безопасности, относящихся к КВОИ, в соответствии с установленными процедурами.

в) мероприятия по реагированию на инциденты безопасности КВОИ: необходимо определить мероприятия по реагированию на инциденты, относящиеся к КВОИ, включая роли и обязанности группы реагирования на инциденты, целесообразные и эффективные процедуры управления операциями и эффективно работающие, настроенные средства защиты; планы при обострениях событий; первоочередные действия, которые необходимо предпринять при обнаружении вторжения и связанную с ними ответственность за оценку последствий; контрмеры, необходимые для смягчения последствий и восстановления функционирования КВОИ до безопасного эксплуатационного состояния.

**12.5** Мероприятия по реализации требований к планированию реагирования на инциденты, связанные с нарушением безопасной эксплуатации КВОИ выполняются под руководством ответственного лица, на которое возлагаются следующие обязанности:

а) вести документацию, которая определяет классификацию инцидентов, мероприятия по реагированию на физические инциденты и требования к сообщениям об инцидентах информационной безопасности;

б) хранить протоколы о физических и информационных инцидентах в течение трех календарных месяцев;

в) демонстрировать в ходе контроля безопасности КВОИ соответствие мер по управлению инцидентами установленным требованиям через самооценку, предоставляемую ежегодно эксперту по соответствию. Аудитор может также использовать плановые проверки на местах каждые три года и расследования при рекламациях для оценки выполнения;

г) хранить в соответствии с законодательством (не менее трех календарных лет) записи, относящиеся к инцидентам физической и сетевой безопасности КВОИ, включающие, как минимум:

– вхождение в файлы регистрации системные и приложений, относящиеся к инциденту;

– записи видео и/или физического доступа, относящиеся к инциденту;

– документированные записи выполняемых расследований и анализа;

– записи обо всех доложенных инцидентах и последовавших докладов;

д) сделать все записи и документацию доступными для проверки экспертом по соответствию по его запросу.

**12.6** Внешний аудитор должен хранить записи аудита в соответствии с законодательством (не менее трех лет).

## 13 Разработка и реализация планов восстановления после инцидентов

**13.1** Владелец объекта КИ должен разработать план восстановления нормального функционирования КВОИ и иметь в наличии ресурсы, необходимые для успешной его реализации, если это будет необходимо.

**13.2** Планы восстановления должны разрабатываться с учетом того, что КВОИ или их отказавшие компоненты не могут быть немедленно и полностью восстановлены (заменены) и быть рассчитаны на события различной длительности и тяжести, с учетом установленных требований к непрерывности операций и процессов объекта инфраструктуры и методам и мерам восстановления КВОИ при авариях.

**13.3** Процедуры реагирования и восстановления должны быть ясными, точными, целесообразными и выполнимыми. В противном случае возможен высокий риск того, что они могут быть неверно истолкованы, проигнорированы или обойдены.

**13.4** Планы восстановления КВОИ должны анализироваться и периодически корректироваться, включать обязанности по постоянному отслеживанию:

- новых организационных, организационно-технических и физических мер обеспечения безопасности КВОИ;

- современных версий физических и программно-аппаратных средств для их реализации, чтобы гарантировать их постоянную эффективность.

Периодичность корректировки плана должна соответствовать длительности, тяжести и вероятности каждого вида инцидентов.

Примечание – Например, событие с более высокой вероятностью при короткой длительности может не потребовать тренировок по плану восстановления вообще, поскольку владелец регулярно на него реагирует. Однако план восстановления КВОИ при более низкой вероятности события с тяжелыми последствиями должен предусматривать тренировки, которые должны проводиться, как минимум, ежегодно.

**13.5** Для сопровождения планов восстановления необходимо:

- а) разработать планы восстановления нормального функционирования КВОИ и пересматривать эти планы ежегодно;

- б) определить конкретные способы реагирования на инциденты различной длительности и тяжести, которые могут привести в действие планы восстановления;

- в) обновлять планы восстановления в пределах 30 дней со дня изменений в КВОИ или процедурах безопасности - по мере необходимости, и вносить в план восстановления контактную информацию;

- г) разработать план тренировок в соответствии с планом восстановления КВОИ, который будет включен в программу тренировок и повышения квалификации персонала ("изучение уроков").

**13.6** Обязанности по реализации требований к планированию восстановления КВОИ после инцидентов включают следующее:

- а) ОДЛ должно:

- оформить документально план восстановления КВОИ после инцидентов и поддерживать записи всех уроков или тренировок за последние три года;

- анализировать и корректировать план в отношении реагирования на инциденты различной длительности и тяжести ежегодно или по необходимости;

- при необходимости изменений в КВОИ или процедурах безопасности анализировать, обновлять, документировать и вносить изменения в планы восстановления в течение 30 дней;

- проводить и поддерживать отчеты об обучении персонала в соответствии с планами восстановления, по крайней мере, каждые три года или по необходимости;

- б) при контроле безопасности КВОИ ОДЛ должно продемонстрировать соответствие мер по планированию восстановления после инцидентов установленным требованиям через самооценку, представляемую эксперту по соответствию ежегодно. Эксперт по соответствию может также запланировать ревизии на местах каждые три года и расследования по претензиям, чтобы оценить выполнение этих требований;

- в) период проверки эффективности плана восстановления должен составлять один календарный год. Ответственное лицо должно сохранять данные проверок в течение трех календарных лет. Аудитор должен хранить данные записей аудита в течение трех лет;

- г) ответственное лицо должно обеспечить доступность для проверки необходимых документов по запросу эксперта по соответствию.

## 14 Обеспечение надежного функционирования КВОИ в процессе эксплуатации

### 14.1 Обеспечение надежного функционирования КВОИ на этапах его жизненного цикла

**14.1.1** Обеспечение надежного функционирования КВОИ в процессе эксплуатации должно предусматриваться на всех этапах его жизненного цикла – проектирования, разработки, создания, ввода в эксплуатацию.

**14.1.2** На этапе проектирования для обеспечения надежного функционирования КВОИ должны применяться следующие основные правила:

а) проект КВОИ не должен содержать необоснованной сложности ни в его функциональных возможностях, ни в их реализации. Демонстрация этого является важной для безопасности, так как использование цифровых технологий программирования позволяет обеспечить достаточно сложный состав функций. Частью этой демонстрации должно быть свидетельство о следовании структурированному проектированию, культуре программирования и правилам кодирования;

б) функциональные требования для систем безопасности КВОИ, выполняемые компьютерной системой, должны быть существенно важными для обеспечения функционирования объекта инфраструктуры. Функции, не затрагивающие безопасность функционирования объекта по существу, должны быть отделены от основных функций, и должно быть показано, что они не влияют на них;

в) при разработке системы безопасности КВОИ на основе СВТ во избежание проблем неизбежной сложности целесообразно использовать концепцию декомпозиции "сверху вниз" и модульной структуры. Они позволяют разработчику системы защиты заниматься несколько меньшими и более управляемыми задачами и обеспечивают более эффективный анализ качества системы защиты при проведении ее контроля. Логика при разделении системы защиты на модули и описание интерфейсов должны быть, насколько возможно, простыми;

г) при проектировании системных модулей предпочтение должно отдаваться более простым алгоритмам. Для программно-аппаратных средств, используемых в системах безопасности, должны быть точно указаны необходимая мощность и пропускная способность;

д) должны быть предусмотрены следующие меры, обеспечивающие надежную эксплуатацию КВОИ:

1) защита информации о технических средствах и КВОИ в целом, в том числе назначение и перечень решаемых задач; номенклатура и объем обрабатываемой информации; время решения типовых информационных и расчетных задач; используемые средства и способы защиты информации и другие сведения;

2) резервирование средств КВОИ:

– резервирование ТС и источников первичного питания КВОИ;

– резервирование документации на КВОИ;

– резервирование информационных массивов и доступ пользователей КВОИ в соответствии с их полномочиями и установленными правилами разграничения доступа;

3) использование конструктивных особенностей, повышающих надежность:

– применение принципа диверсификации (разнотипности) компонентов и функций КВОИ, снижающей возможность отказов ПО по общей причине.

Примечание – Необходимо рассматривать возможность использования диверсификации на различных уровнях проекта. Должна быть также учтена диверсификация методов, языков, инструментов и персонала. Следует заметить, что, хотя диверсификация ПО может повысить защиту от ошибок ПО обычного вида, она не гарантирует отсутствие сопутствующих ошибок. Решение об использовании принципа диверсификации, выбор типа или решение не использовать разнотипность должно быть обосновано разработчиком;

4) в ПО должны быть добавлены средства обеспечения безопасного отказа КВОИ, диспетчерского управления и механизмы, обеспечивающие устойчивость к отказам, в объеме, в котором дополнительная сложность оправдывается очевидным общим повышением безопасности;

5) должно быть предусмотрено использование внешних устройств, таких, как датчики времени систем безопасности, что реакцию КВОИ на обнаружение неисправности более надежной;

б) непосредственно к случайным отказам аппаратного обеспечения КВОИ должен применяться критерий единичного отказа: один отказ не должен приводить к потере функций, обеспечивающих безопасность функционирования КВОИ;

е) в процессе проектирования и разработки КВОИ для определения важности его функций должна использоваться схема их классификации по уровням безопасности. Она концентрирует внимание проектировщиков объекта инфраструктуры, операторов и специалистов на спецификациях, проекте, квалификации, проверке качества, изготовлении, установке, обслуживании и тестировании систем и оборудования, которые гарантируют безопасность. Ранжированные требования к проектированию и характеристикам применительно к функциям компьютерной системы могут быть взяты из схемы классификации КВОИ по безопасности. КВОИ должен соответствовать критериям самого высокого класса безопасности функций, которые он реализует;

Система защиты КВОИ, нарушение безопасности которых может привести к высокому или катастрофическому ущербу, должна отвечать следующим специальным требованиям:

- быть встроенной в КВОИ таким образом, чтобы ее запуск был невозможен в обход средств защиты КВОИ;

- охватывать все элементы КВОИ и осуществлять метод мандатного (принудительного) контроля доступа субъектов к его ресурсам при всех режимах эксплуатации;

- реализовываться на основе специальных программных и аппаратных средств, разработанных по заказу, или средств, сертифицированных органом, уполномоченным на сертификацию систем и средств защиты ИТ систем и изделий по специальным стандартам;

- при проектировании и разработке системы защиты КВОИ должен обеспечиваться режим секретности;

ж) на каждом этапе проектирования системы и связанного с нею ПО должен тщательно оцениваться компромисс в достижении различных противоречивых целей проекта. При этом должен обеспечиваться баланс между снижением риска нарушения безопасности КВОИ и объемом работ по защите его ресурсов.

**14.1.3** На этапе изготовления надежность КВОИ должна обеспечиваться отбором надежных компонент для его создания и тщательным тестированием его подсистем до ввода в эксплуатацию.

Ввиду сложности, а иногда невозможности проведения классических испытаний КВОИ на надежность, оценка надежности проводится по результатам имитационного моделирования отказов КВОИ или расчетным путем.

Тестирование и проверка надежности программ специального ПО должна проводиться по специально разработанной методике, обеспечивающей проверку выполнения требований о защите авторских прав, защите охраняемой информации, корректности выполнения задач.

Все программные и технические средства КВОИ должны пройти проверку на возможное наличие встроенных элементов перехвата, искажения, передачи и уничтожения обрабатываемой информации.

Должна быть продемонстрирована способность ПО, используемого для контроля аппаратных средств КВОИ, корректно реагировать на все отклонения от нормального функционирования в процессе их работы.

**14.1.4** На этапе ввода в эксплуатацию надежность КВОИ должна подтверждаться через тестирование подсистем КВОИ, аттестацию системы защиты и использование сертифицированных средств защиты КВОИ в соответствии с установленным порядком.

**14.1.5** На этапе эксплуатации КВОИ должно обеспечиваться надежное оперативное управление его безопасностью, включающее:

- своевременное проведение работ по сопровождению и обслуживанию реализующих его компонентов или обеспечение "горячего" или "холодного" резервирования;

- контроль действий пользователей с целью обнаружения в реальном времени нарушений правил обмена информацией, качества и полноты информации, хищений информации, потери ее целостности, несанкционированного доступа к информационным и вычислительным ресурсам КВОИ;

- оперативное реагирование на попытки реализовать угрозы и нарушение защиты КВОИ (действия внутреннего нарушителя, внешние атаки и т.п.);

- распознавание субъекта, вызвавшего нарушение защиты КВОИ;

- быстрое восстановление нарушенных функций КВОИ;
- записи в журнале аудита (собственная история КВОИ) для исследования причин отказов и принятия соответствующих мер по повышению его надежности.

## 14.2 Требования к надежности технических средств и оборудования

14.2.1 Для обеспечения надежного функционирования КВОИ должны выполняться следующие требования:

- а) ТС и оборудование должно выбираться исходя из:
  - их соответствия решаемым задачам и выбранной базовой программной платформе КВОИ;
  - соотношения стоимость/производительность;
  - степени возможности их приобретения в Республике Беларусь (для исключения проблем с заменой комплектующих и поиском персонала для технического сопровождения);
  - наличия долгосрочной перспективы серийного промышленного производства и поставщиков;
  - других причин;
- б) среда функционирования стандартных средств и оборудования КВОИ должна соответствовать следующим требованиям:
  - ТС следует устанавливать в закрытых отапливаемых помещениях;
  - в окружающей среде не должно быть паров агрессивных веществ, вызывающих коррозию;
  - температура окружающего воздуха от 10 до 35 °С;
  - относительная влажность окружающего воздуха от 40 до 80 % при температуре окружающего воздуха 30 °С;
  - атмосферное давление от 84 до 107 кПа (от 630 до 800 мм рт. ст.);
  - электропитание осуществляется от однофазной сети переменного тока напряжением 230 В с отклонением  $\pm 10$  %, частотой (50  $\pm 1$ ) Гц;
  - напряженность внешнего электромагнитного поля должна быть не более 3 В/м в диапазоне частот от 0,15 до 300 МГц;
- в) монтаж ТС КВОИ должен соответствовать следующим требованиям:
  - для электропитания рабочих станций необходимо использовать отдельную электролинию, к которой не должно подключаться силовое и коммутационное электрооборудование. В сети не должно быть импульсных помех, сбоев электропитания;
  - электропитание систем КВОИ должно осуществляться через источник бесперебойного питания;
  - должны быть выполнены требования защиты КВОИ от утечки информации по техническим каналам;
  - использование сетевых ТС и оборудования должно соответствовать общепринятым промышленным ТНПА для объектов электросвязи;
  - технические характеристики и электрические параметры цепей стыка каналов и трактов, используемых в сети передачи данных и на КВОИ должны соответствовать ТНПА для аналоговых и цифровых систем передачи;
  - показатели надежности на цифровые каналы и тракты первичной сети передачи данных с коммутацией пакетов, а также методы их измерений автоматизированным способом определяются и регламентируются в соответствии с государственными ТНПА.
  - сигнальные линии локальной сети прокладываются (с резервированием) двумя кабелями с уточнением дополнительных параметров, специфичных для условий эксплуатации КВОИ;
  - трассы линий связи должны пролегать в отдельных кабельных зонах, исключая взаимодействие с силовыми линиями электропитания.
  - связи между КВОИ для передачи информации ограниченного доступа должны осуществляться через сетевые маршрутизаторы, обеспечивающие разделение информационных потоков и защиту информации от НСД при ее передаче от одной рабочей станции к другой.

**14.2.2** Если по условиям технологического процесса выполнить какие-либо из приведенных требований не представляется возможным, решения по выбору типа ТС, оборудования и их защите принимаются исходя из конкретных условий.

### **14.3 Требования к надежности программного обеспечения**

**14.3.1** Надежность ПО характеризуется способностью программных средств в конкретных областях применения выполнять заданные функции в соответствии с программной документацией в условиях отклонений в среде эксплуатации, вызванных сбоями ТС, ошибками входных данных, ошибками обслуживания и другими дестабилизирующими воздействиями согласно СТБ П 34.101.39.

**14.3.2** ПО КВОИ должно обеспечивать его отладку, функционирование, проверку работоспособности и включать:

- общесистемное ПО – операционные системы, в состав которых входят системы управления вычислительными процессами, системы управления базами данных, а также стандартные пакеты и утилиты для обеспечения удобства работы операционной системы в качестве прикладного ПО;

- специальное ПО – совокупность программ, разработанных для реализации задач конкретного КВОИ.

**14.3.3** Для обеспечения надежного функционирования ПО КВОИ в среде эксплуатации необходимо руководствоваться следующими положениями:

- при выборе (разработке) ПО должна использоваться технология эволюционирующих прототипов, обеспечивающая планомерное наращивание возможностей разрабатываемых программных комплексов без их радикальной переработки;

- ПО должно разрабатываться как открытая система, позволяющая изменять его состав и структуру связей между блоками;

- ПО должно обеспечивать решение прикладных задач как в сетевом, так и в автономном режимах функционирования КВОИ;

- перечень базовых инструментальных средств, используемых при разработке прикладного ПО, уточняется в ходе сертификации ПС. Предлагаемый инструментарий должен обеспечить использование специального ПО без существенных переработок;

- перечень инструментальных средств определяется исходя из требований по установке и эксплуатации ПО;

- отладка, испытания и сдача в эксплуатацию ПО должны проводиться с использованием условно-реальных исходных данных КВОИ без заполнения баз данных истинной информацией;

- при разработке и отладке специального ПО должна быть обеспечена защита информации КВОИ от утечки по каналам ПЭМИН, от НСД, от специальных программно-математических воздействий ("вирусов");

- базовое ПО КВОИ должно быть сертифицировано по требованиям ТНПА по защите информации;

- программные продукты, используемые в составе ПО КВОИ, должны иметь лицензию. До их встраивания в состав ПО КВОИ должна быть проведена их аттестация или сертификация на соответствие требованиям безопасности в национальной системе оценки соответствия.

**14.3.4** Архитектура общего ПО КВОИ должна представляться в виде иерархии уровней программных средств, каждый из которых выполняет определенные функции по сбору, передаче, хранению, обработке и представлению информации и, кроме того, предоставляет услуги более верхнему уровню для выполнения им своих функций. Каждый уровень должен иметь строго определенный (стандартный) интерфейс для организации взаимодействия программных средств различных уровней и подключения новых программных средств.

**14.3.5** Математическое обеспечение КВОИ, представленное совокупностью применяемых математических методов, моделей и алгоритмов обработки данных, должно включать следующие элементы:

- базы данных, содержащие информацию о силах, средствах и аппаратуре защищаемых КВОИ в объеме, достаточном для проведения расчетов и принятия решений;

- базы данных, содержащие информацию о результатах проверок КВОИ и принятых мерах;
- базы данных, содержащие информацию о ходе эксплуатации КВОИ, планах модернизации;
- базы данных – архивы (повседневный документооборот, руководящие документы, НПА, решения и т.д.);
- комплексы информационных задач, обеспечивающих подготовку по установленным формам справок по материалам перечисленных баз данных и массивов исходных данных для автоматизированных расчетов;
- комплексы расчетных задач, разрабатываемые в соответствии с утвержденными постановками задач, обеспечивающие оценку защиты КВОИ, организационных мероприятий, прогнозирование направлений развития и ожидаемых результатов.

При разработке математического обеспечения должен максимально использоваться блочно-модульный принцип построения прикладных программ и комплексов программ, обеспечивающих проведение доработок математического обеспечения с минимальными трудозатратами.

Разработка математического обеспечения КВОИ должна предусматривать возможность работы с задачами в автономном режиме при отказе сетевого оборудования или выходе из строя файловых серверов (без использования баз данных, где это возможно), а также обмен данными между задачами с использованием в качестве промежуточного носителя жесткого магнитного диска одной из рабочих станций КВОИ или гибких магнитных дисков.

### **15 Техническое обследование критически важных объектов информатизации для оценки соответствия состояния технической защиты информации установленным требованиям**

**15.1** Техническое обследование КВОИ по требованиям ТЗИ проводится в форме проверок, проводимых специально сформированной комиссией.

Техническое обследование включает:

- предварительное ознакомление с КВОИ – объектом технического обследования;
- проведение необходимых работ по техническому обследованию КВОИ;
- оформление и выдачу "Заключения по результатам технического обследования КВОИ по требованиям ТЗИ".

**15.2** Предварительное ознакомление с КВОИ – объектом технического обследования осуществляется, как правило, без выезда непосредственно на объект путем изучения соответствующих информационных материалов, включающих, в частности, уровень важности КВОИ, перечень актуальных угроз (разрабатывается организацией, ответственной за эксплуатацию КВОИ, и согласовывается с Оперативно-аналитическим центром при Президенте Республики Беларусь).

**15.3** В процессе проведения технического обследования КВОИ осуществляется выполнение следующих основных работ:

- анализ состава и структуры комплекса технических средств, ПО и информационных потоков в процессе функционирования КВОИ, с точки зрения ТЗИ;
- анализ состава и структуры системы (подсистемы) информационной безопасности;
- проведение испытаний средств и элементов систем (подсистем) информационной безопасности на обследуемых объектах КВОИ с помощью контрольной аппаратуры и тестовых средств;
- анализ результатов испытаний средств защиты;
- техническое обследование КВОИ в реальных условиях эксплуатации путем проверки фактического состояния ТЗИ на объектах КВОИ на различных этапах технологического процесса;
- оформление документов по результатам технического обследования.

**15.4** В ходе анализа состава и структуры комплекса технических средств, ПО и информационных потоков на КВОИ осуществляется:

- анализ характеристик комплекса основных и вспомогательных технических средств, ПО, их режимов работы, основных этапов технологического процесса обработки информации и выявление уязвимостей;

- анализ конфигурации и топологии КВОИ в целом и его отдельных компонентов, физические, функциональные и технологические связи внутри КВОИ и с другими системами различного уровня и назначения;

- анализ режимов обработки информации в КВОИ в целом и на отдельных объектах КИ;

- анализ состояния защищенности аппаратных и программных средств объектов КВОИ от угроз нарушения ТЗИ.

**15.5** В ходе анализа состава и структуры системы (подсистемы) защиты информации КВОИ осуществляется:

- анализ номенклатуры и содержания решаемых задач системой ТЗИ;

- анализ номенклатуры и степени соответствия используемых технических и программных средств ТЗИ предъявляемым требованиям;

- анализ алгоритмов функционирования системы ТЗИ, в том числе – при внезапном возникновении различных угроз безопасности информации.

**15.6** При проведении испытаний средств и элементов систем (подсистем) ТЗИ на обследуемых объектах КВОИ с помощью контрольной аппаратуры и тестовых средств не допускается использование режимов тестирования, являющихся потенциально опасными с точки зрения обеспечения бесперебойного функционирования КВОИ, без письменного разрешения организации, ответственной за его эксплуатацию.

**15.7** В процессе проведения анализа результатов испытаний средств ТЗИ осуществляется:

- сравнение реальных характеристик средств защиты с указанными в документации на средства защиты и в требованиях на обеспечение ТЗИ на объектах КВОИ;

- определение достаточности состава средств защиты, используемых на объектах КВОИ для обеспечения ТЗИ;

- при необходимости, составление перечня сертифицированных средств ТЗИ, предлагаемого для использования на объектах КВОИ.

**15.8** Техническое обследование КВОИ по требованиям ТЗИ проводится на следующих стадиях их жизненного цикла:

а) в процессе ввода в эксплуатацию создаваемых или модернизируемых КВОИ выполняется:

- проверка выполнения требований ТЗИ на объектах КВОИ при опытной эксплуатации средств ТЗИ в комплексе с другими техническими и программными средствами КВОИ;

- проверка соответствия результатов приемо-сдаточных испытаний средств ТЗИ по результатам опытной эксплуатации требованиям нормативно-методических документов и технического задания;

б) на стадии модернизации КВОИ выполняется:

- проверка соответствия организационно-технических мероприятий по защите информации предъявляемым требованиям;

- соответствие организации охраны и физической защиты помещений КВОИ требованиям ТЗИ, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

- проверка соответствия проекта строительных, строительно-монтажных работ (при реконструкции КВОИ) ТТЗ (ТЗ) на разработку системы (подсистемы) информационной безопасности.

**15.9** При проведении технического обследования действующего КВОИ, не подвергавшегося техническому обследованию на этапах ввода в эксплуатацию и модернизации, необходимо проведение всего комплекса работ.

**15.10** При оформлении документов по результатам технического обследования КВОИ на соответствие требованиям ТЗИ в общем случае осуществляется:

- оформление актов и протоколов испытаний аппаратных и программных средств объектов КВОИ на защищенность от угроз информационной безопасности;

- оформление актов и протоколов испытаний аппаратных и программных средств защиты информации;
- оформление заключений по каждой из работ, проведенных в соответствии с программой технического обследования;
- формирование заключения по результатам технического обследования КВОИ на соответствие требованиям ТЗИ.

**15.11** Заключение по результатам технического обследования КВОИ по требованиям ТЗИ выдается на три года и включает:

- характеристику состава аппаратных и программных средств КВОИ и результаты анализа их уязвимости с точки зрения информационной безопасности;
- характеристику организационной структуры и уровня подготовки специалистов, ответственных за ТЗИ на КВОИ;
- характеристику состава применяемых аппаратных и программных средств ТЗИ;
- выводы по результатам проведения работ, включенных в программу испытаний со ссылками на приложения (акты и протоколы технических испытаний);
- перечень выявленных недостатков ТЗИ и рекомендации по их устранению с указанием сроков проведения работ и минимально необходимого их объема;
- рекомендации по совершенствованию системы ТЗИ;
- вывод о возможности дальнейшей эксплуатации КВОИ и сроках проведения повторного обследования.

К заключению прилагаются акты и протоколы технических испытаний, содержащие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Указанные документы подписываются членами комиссии, проводившими измерения (испытания) и утверждаются ее руководителем.

Заключение по результатам технического обследования КВОИ по требованиям ТЗИ формируется и подписывается председателем комиссии, всеми членами комиссии и представляется на утверждение в соответствующее отраслевое Министерство.

Утвержденное заключение в установленном порядке передается в Оперативно-аналитический центр при Президенте Республики Беларусь. Один экземпляр заключения после утверждения передается организации, ответственной за эксплуатацию КВОИ.

**15.12** При несоответствии КВОИ требованиям ТЗИ и невозможности оперативного устранения отмеченных недостатков Оперативно-аналитический центр при Президенте Республики Беларусь сообщает об отказе в выдаче Заключения. При этом может быть предложен срок повторного технического обследования при условии устранения недостатков. При наличии замечаний непринципиального характера Заключение может быть выдано после проверки, подтверждающей устранение недостатков.

**15.13** Оперативно-аналитический центр при Президенте Республики Беларусь осуществляет ведение базы данных по КВОИ, прошедших техническое обследование, с целью совершенствования ТЗИ создаваемых и действующих КВОИ и планирования мероприятий по контролю и надзору за их состоянием.

**15.14** Организации, ответственные за эксплуатацию и за техническое обследование КВОИ, несут партнерскую ответственность за качество ТЗИ на КВОИ, получившего Заключение.

**15.15** В случае изменения условий функционирования и/или технологии обработки информации организация, ответственная за эксплуатацию КВОИ, прошедшего техническое обследование на соответствие требованиям ТЗИ, обязана известить об этом Оперативно-аналитический центр при Президенте Республики Беларусь, который принимает решение о необходимости проведения дополнительных проверок системы ТЗИ на КВОИ.

## **16 Идентификация критически важных объектов информатизации критической инфраструктуры**

**16.1** Для выделения КВОИ из состава объектов информатизации необходимо обеспечить инвентаризацию критичных активов объекта КИ, включающих устройства, системы и оборудование, выход из строя, разрушение, снижение качества функционирования или отказ которых иметь отрицательное воздействие на важнейшие процессы объекта инфраструктуры, привести к чрезвычайной ситуации техногенного характера или к значительным негативным последствиям для безопасности в политической, экономической, социальной, информационной, экологической и иных сферах.

Идентификация КВОИ объекта КИ должна осуществляться на основе оценки возможных последствий (ущерба) и приемлемых рисков нарушения функционирования объекта КИ при нарушении функционирования или отказе ОИ.

ОИ, идентифицированный как критически важный, заносится в список КВОИ и подлежит регистрации в ведомственном и/или государственном перечнях КВОИ.

**16.2** Мероприятия по идентификации КВОИ объекта КИ включают:

- оценку риска нарушения безопасности объекта КИ при отказе ОИ;
- составление и сопровождение документации, отражающей оценки риска, использованные при идентификации КВОИ. Документация должна включать описание методологии аудита при оценке риска, критерии и процедуры оценки;
- утверждение списка критичных активов объекта инфраструктуры и соответствующих им КВОИ с указанием даты утверждения;
- поддержку утвержденного перечня КВОИ объекта КИ (составление, актуализация);
- поддержку документации по всем КВОИ в соответствии с утвержденным перечнем;
- направление документации на идентифицированные КВОИ в вышестоящую организацию для рассмотрения и регистрации в ведомственном и/или государственном Перечне КВОИ в соответствии с законодательством;
- организация внутреннего контроля безопасности КВОИ с целью анализа его защищенности.

### Библиография

- [1] ИСО/МЭК 2382-8:1998 Информационная технология. Словарь. Безопасность
- [2] ISO/IEC GUIDE 2:2004(E/F/R) Стандартизация и смежные виды деятельности. Общий словарь
- [3] Положение об отнесении объектов информатизации к критически важным, организации функционирования и обеспечения безопасности критически важных объектов информатизации  
Утверждено Указом Президента Республики Беларусь "О некоторых мерах по обеспечению безопасности критически важных объектов информатизации" (проект)
- [4] Положение о порядке защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено  
Утверждено постановлением Совета Министров Республики Беларусь от 26 мая 2009 г. № 675

Начальник центра испытаний средств  
защиты информации и аттестации  
информационных объектов

О.Ю.Кондрахин

Исполнители:

Ведущий научный сотрудник

Э.П.Крюкова

Старший научный сотрудник

В.А.Дмитриев

Инженер 1-й категории

М.К.Андрухович

Инженер 2-й категории

Е.А.Доценко

Инженер

М.Ю.Казеев

Ведущий инженер  
по стандартизации

В.М.Кравцова