ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

**СТБ 2105-2012**

## Информационные технологии

# ИНТЕРНЕТ-САЙТЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНИЗАЦИЙ

**Требования**

## Інфармацыйныя тэхналогіі

# ІНТЭРНЭТ-САЙТЫ ДЗЯРЖАЎНЫХ ОРГАНАЎ І АРГАНІЗАЦЫЙ

**Патрабаванні**

**Издание официальное**

**Госстандарт**

**Минск**

УДК 004.774.6(083.74)(476) МКС 35.020 КП 05

**Ключевые слова:** интернет-сайт, государственный орган, государственная организация

## 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 открытым акционерным обществом «Гипросвязь» (ОАО «Гипросвязь»)
ВНЕСЕН Министерством связи и информатизации Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от 13 декабря 2012 г. № 79

3 ВЗАМЕН СТБ П 2105-2010



Издан на русском языке

## Содержание

**ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ**

# Информационные технологии
# ИНТЕРНЕТ-САЙТЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНИЗАЦИЙ
# Требования

# Інфармацыйныя тэхналогіі
# ІНТЭРНЭТ-САЙТЫ ДЗЯРЖАЎНЫХ ОРГАНАЎ І АРГАНІЗАЦЫЙ
# Патрабаванні

Information technologies
Internet-sites of state bodies and organizations
Requirements

**Дата введения 2013-03-01**

## 1 Область применения

Настоящий стандарт устанавливает требования к разработке, дизайну, регистрации и размещению интернет-сайтов государственных органов и организаций (далее – интернет-сайты), а также требования по защите информации для центров обработки данных, осуществляющих услуги хостинга для интернет-сайтов государственных органов и организаций.

Настоящий стандарт предназначен для применения при разработке, сопровождении, эксплуатации и размещении интернет-сайтов государственных органов и организаций.

## 2 Нормативные ссылки

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

СТБ 34.101.37-2011 Информационные технологии. Методы и средства безопасности. Профиль защиты программных средств. Системы управления сайта

СТБ 982-94 Информационная технология. Термины и определения

СТБ 1439-2008 Услуги электросвязи. Термины и определения

СТБ 1693-2009 Информатизация. Термины и определения

ГОСТ ИСО/МЭК 2382-1-99 Информационная технология. Словарь. Часть 1. Основные термины

Примечание – При пользовании настоящим стандартом 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 стандартом 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 стандарте применяют термины, установленные в [1], СТБ 982, СТБ 1439, СТБ 1693, ГОСТ ИСО/МЭК 2382-1, а также следующие термины с соответствующими определениями:

**3.1 активы интернет-сайта:** Совокупность программных средств, предназначенных для обеспечения функционирования центра хранения и обработки данных.

**3.2 безопасность информации:** Состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т. е. сохранение информации в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

**3.3 веб-браузер:** Специальное программное средство просмотра веб-страниц.

**3.4 государственные органы и организации:** Республиканские органы государственного управления, местные исполнительные и распорядительные органы, иные государственные органы и государственные организации, а также хозяйственные общества, в отношении которых Республика Беларусь

Издание официальное

либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами.

**3.5 защита информации от несанкционированного доступа (защита от НСД) или воздействия:** Деятельность, направленная на предотвращение получения информации (или воздействия на информацию) заинтересованным субъектом с нарушением установленных прав или правил.

**3.6 интернет-сайт:** Веб-сайт, размещенный в сети Интернет.

**3.7 интернет-сервер:** Программно-аппаратные средства, входящие в состав сети Интернет и реализующие определенные функции (хранение, обработка, передача информации и т. п.).

**3.8 система защиты информации:** Комплекс организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации.

**3.9 узел доступа:** Технические ресурсы информационной системы, через которые осуществляется доступ к сетям общего пользования.

**3.10 центр обработки данных:** Помещение (площадка), специально оборудованная для размещения серверного и коммуникационного оборудования и подключения к каналам сети Интернет.

## 4 Сокращения

В настоящем стандарте используются следующие сокращения:

АРМ – автоматизированное рабочее место;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ОАЦ – Оперативно-аналитический центр при Президенте Республики Беларусь;

ОС – операционная система;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

СВТ – средства вычислительной техники;

DCE/RPC – Distributed Computing Environment/Remote Procedure Calls – бинарный протокол на базе различных транспортных протоколов;

FTP – File Transfer Protocol – протокол передачи файлов;

ICMP – Internet Control Message Protocol – межсетевой протокол управляющих сообщений;

SMTP – Simple Mail Transfer Protocol – простой протокол передачи почты;

SMS – System Management Server – сервер управления системой;

W3C – World Wide Web Consortium – консорциум Всемирной паутины;

WAI – Web Accessibility Initiative – инициатива по обеспечению доступности Web;

WCAG – Web Content Accessibility Guidelines – руководство по обеспечению доступности содержимого;

HTML – HyperText Markup Language – язык разметки гипертекста;

URL – Uniform Resource Locator – универсальный локатор ресурса (адрес страницы интернет-сайта).

## 5 Требования к разработке и дизайну интернет-сайта

### 5.1 Соответствие международным стандартам и рекомендациям

**5.1.1** Интернет-сайт должен соответствовать спецификациям и рекомендациям W3C.

**5.1.2** Информация, размещенная на интернет-сайте, должна быть доступна для пользователей независимо от уровня их образования и технической подготовки. Должна быть предусмотрена версия интернет-сайта для слабовидящих пользователей. Дизайн интернет-сайтов должен разрабатываться с учетом рекомендаций W3C WAI-WCAG.

### 5.2 Требования к навигации по интернет-сайту

**5.2.1** Для обеспечения первоочередной загрузки важнейших элементов на странице интернет-сайта и их доступности необходимо размещать основные навигационные ссылки в верхней части каждой страницы интернет-сайта. Выбранный и определенный порядок навигации должен соблюдаться на каждой странице интернет-сайта.

**5.2.2** Вся информация, размещенная на интернет-сайте должна быть доступна посетителю через ссылку или пункт меню. Количество переходов по элементам навигации для доступа к запрашиваемой информации не должно превышать пяти. Навигационные элементы должны выделяться на фоне остальных элементов интернет-сайта.

Для представления элементов системы навигации по интернет-сайту рекомендуется использовать текстовое меню, не рекомендуется использовать JavaScript и Flash-анимацию.

Каждая гиперссылка должна быть рабочей и приводить пользователя к ожидаемому им ресурсу. В случае, если дается гиперссылка на внешний интернет-сайт, рекомендуется, чтобы оповещение об этом пользователя осуществлялось заранее, при этом страницы, на которые указывают такие гиперссылки, должны открываться в новом окне веб-браузера. Если гиперссылка используется для загрузки файла, рекомендуется указывать его тип и размер.

**5.2.3** Необходимо использовать навигационные цепочки, содержащие путь следования по разделам от главной страницы интернет-сайта до текущей открытой страницы.

**5.2.4** Для интернет-сайтов, содержащих большие объемы информации, необходимо предусмотреть наличие дополнительных навигационных элементов, таких как:

– указатели (алфавитный, тематический и т. п.), представляющие собой подборку ссылок на страницы интернет-сайта, сгруппированных по различным критериям;

– ссылки на самые посещаемые страницы интернет-сайта или недавно добавленные документы.

При размещении на странице интернет-сайта большого объема текстовой информации необходимо использовать внутренние ссылки (якоря) на различные разделы страницы. В свою очередь, в каждом разделе страницы должна быть ссылка «Вернуться в начало», позволяющая пользователю вернуться к началу страницы.

### 5.3 Требования к механизму поиска для интернет-сайта

**5.3.1** Форма поиска либо ссылка на нее должна быть доступна на каждой странице интернет-сайта. Поле для ввода поискового запроса должно обеспечивать ввод не менее 20 символов.

**5.3.2** При размещении на интернет-сайте информационного (ых) ресурса (ов) необходимо реализовать функцию расширенного поиска либо поиска по размещенному (ым) информационному (ым) ресурсу (ам).

**5.3.3** Результаты поиска должны выводиться на отдельной странице, имеющей соответствующий заголовок, при этом поисковый запрос должен оставаться в строке поиска.

На странице вывода результатов поиска должен быть отображен список найденных документов, а также ссылка на форму расширенного поиска (при ее наличии на интернет-сайте).

По умолчанию список результатов поиска должен быть отсортирован по релевантности. Каждый пункт в списке должен содержать ссылку на страницу интернет-сайта и фрагмент текста, в котором выделены ключевые слова, заданные в поисковом запросе.

В результатах поиска для каждого документа должна быть указана дата его обновления.

Если результат поиска относится не к HTML-странице, то рядом со ссылкой на такой документ необходимо указать его формат и размер.

**5.3.4** Если в результате поиска не были найдены документы, удовлетворяющие поисковому запросу, то пользователь должен быть проинформирован об этом соответствующим образом, кроме того, на странице должна быть предоставлена краткая информация по улучшению поискового запроса.

### 5.4 Требования к дизайну интернет-сайта

**5.4.1** Все страницы интернет-сайта должны иметь единый дизайн.

Дизайн страниц интернет-сайта должен быть отделен от информационного наполнения и разработан с использованием каскадных таблиц стилей. Должна быть разработана специальная таблица стилей для отображения интернет-сайта с использованием мобильных устройств (PDA-версия интернет-сайта).

**5.4.2** При разработке макета страниц интернет-сайта необходимо придерживаться следующих основных правил:

– шаблон страницы должен обеспечивать корректное восприятие информации при различных размерах окна веб-браузера;

– URL, содержащие статическую информацию, не должны содержать информацию о сеансе работы пользователя с интернет-сайтом;

– на интернет-сайте не должны использоваться фоновые изображения, которые могут затруднить его восприятие или исказить информацию;

– текст должен отображаться с соответствующим уровнем контраста по отношению к используемому цвету фона (не менее 50 %);

– для задания размеров шрифтов, межстрочных интервалов и отступов между абзацами текста необходимо использовать относительные величины;

– необходимо избегать эффектов, затрудняющих восприятие информации или отвлекающих пользователя от содержания документа: мигания и мерцания, эффектов выделения, движущихся строк;

– навигационные и интерактивные элементы страницы (ссылки, изображения, кнопки и т. п.) должны легко идентифицироваться пользователями;

– гиперссылки должны визуально выделяться;

– необходимо применять разные цвета для посещенных и непосещенных ссылок;

– функция печати страниц интернет-сайта должна быть реализована путем разработки специальных таблиц стилей.

**5.4.3** Для упрощения восприятия информации ее рекомендуется разбивать на разделы и подразделы с использованием тегов заголовков (<h>) согласно правилам их использования.

### 5.5 Использование графической и мультимедийной информации

**5.5.1** Файлы графической информации, размещаемой на страницах интернет-сайта, должны храниться в единственном экземпляре в форматах, рекомендованных W3C для использования в сети Интернет и обеспечивающих наименьший объем передаваемых пользователю данных при допустимом уровне качества.

**5.5.2** При размещении графической информации на страницах интернет-сайта необходимо использовать тег альтернативной подписи (<alt>), чтобы она могла быть интерпретирована всеми пользователями. Исключения составляют мелкие декоративные элементы, являющиеся элементами дизайна интернет-сайта или изображения, не несущие смысловой нагрузки и не влияющие на восприятие информации, размещенной на странице.

**5.5.3** Линейные параметры изображения (высота и ширина, координаты позиционирования) должны в обязательном порядке явно определяться в коде разметки страницы.

**5.5.4** Размещаемые на страницах графики или диаграммы необходимо дополнять ссылками на страницы, содержащие соответствующие данные в табличной форме.

**5.5.5** При размещении на странице мультимедийной информации необходимо придерживаться рекомендаций W3C. При использовании мультимедийных элементов, которые отображаются с помощью вспомогательных программ или подключаемых к веб-браузеру модулей, например Flash и QuickTime, необходимо обеспечить альтернативное стандартное представление этих объектов в виде ключевых изображений из анимации или текстового описания. При этом также необходимо убедиться, что информация останется доступной при отключении пользователем отображения мультимедийной информации в веб-браузере.

## 6 Требования к регистрации и размещению интернет-сайта

### 6.1 Общие положения

**6.1.1** Государственные органы регистрируют доменные имена в зонах .gov.by и .mil.by, государственные организации – в зоне .by. Регистрация доменного имени осуществляется в установленном порядке в соответствии с [2].

**6.1.2** Услуги хостинга интернет-сайтов республиканских органов государственного управления оказывают центры обработки данных, имеющие системы управления качеством и информационной безопасностью с соответствующей областью применения.

### 6.2 Технические требования к центрам обработки данных

**6.2.1** Для центров обработки данных должно быть обеспечено наличие:

1) минимум двух каналов доступа в сеть Интернет;

2) минимум двух независимых вводов энергоснабжения;

3) системы кондиционирования холодопроизводительностью не менее 20 % от выделяемой тепловой мощности всех серверов, размещенных в центре обработки данных;

4) резервной системы кондиционирования, позволяющей выдерживать требуемые температуру и влажность в помещениях центра обработки данных в случае отказа основной системы;

5) бесперебойной системы электропитания серверов, позволяющей поддерживать требуемые параметры электропитания на протяжении не менее 2 ч в случае отказа основной системы;

6) системы контроля доступа в помещения центра обработки данных;

7) системы видеонаблюдения в помещениях центра обработки данных;

8) подготовленного персонала в количестве, позволяющем организовать круглосуточное функционирование интернет-сайта.

**6.2.2** Интернет-сайты республиканских органов государственного управления должны быть подключены к ЛВС центра обработки данных на скорости не ниже 10 Мбит/с.

### 6.3 Требования безопасности

#### 6.3.1 Угрозы безопасности и результаты их реализации

**6.3.1.1** Требования безопасности определены с целью предотвращения следующих основных угроз безопасности, возникающих при осуществлении услуг хостинга интернет-сайтов:

– со стороны пользователей сети Интернет в результате их непреднамеренных или умышленных воздействий;

– со стороны персонала интернет-сайта (администраторов, редакторов и др.) в результате их непреднамеренных или умышленных воздействий;

– по причине некорректного функционирования информационной системы;

– в результате чрезвычайных ситуаций (стихийных бедствий и т. п.).

Подробный перечень угроз безопасности интернет-сайта приведен в приложении А.

**6.3.1.2** Результатом реализации вышеперечисленных угроз может являться:

– нарушение целостности (искажение) информации, размещаемой на интернет-сайтах;

– блокирование (недоступность) информации, размещаемой на интернет-сайтах;

– нарушение функций управления интернет-сайтом, в том числе нарушение функций управления средствами обеспечения безопасности интернет-сайта.

#### 6.3.2 Защита активов интернет-сайта

**6.3.2.1** Для обеспечения безопасности активов интернет-сайта и поддержки сетевой инфраструктуры принимаются следующие основные меры:

– активы интернет-сайта должны быть защищены от несанкционированной модификации и не должны содержать пути обхода установленных механизмов контроля;

– ПО сервера устанавливается на выделенном хосте;

– устанавливаются минимально требуемые сервисы сети Интернет;

– устанавливать и конфигурировать программные средства разрешается только системному администратору.

**6.3.2.2** Для обеспечения безопасного функционирования ПО сервера принимаются следующие основные меры:

– своевременное выполнение обновлений;

– удаление или запрещение ненужных сервисов, приложений и примеров содержимого;

– конфигурирование аутентификации пользователей;

– конфигурирование управления ресурсами;

– тестирование безопасности приложений и содержимого;

– постоянный мониторинг поддержки безопасной конфигурации с просмотром журналов аудита и выполнением полного резервного копирования.

**6.3.2.3** ОС должна обеспечивать следующие функции:

– ограничение деятельности административного уровня только авторизованными пользователями;

– управление доступом к данным на сервере;

– запрещение сетевых сервисов, не являющихся необходимыми, встроенных в ПО ОС или сервера;

– управление доступом к различным формам выполнимых программ, таких как CGI-скрипты и плагины, на стороне сервера;

– запись в журнал аудита соответствующей деятельности сервера для определения проникновения и попыток проникновения.

#### 6.3.3 Требования к системе защиты информации

**6.3.3.1** Центр обработки данных должен иметь аттестованную в соответствии с [3] систему защиты информации.

**6.3.3.2** Система защиты информации должна осуществлять функции:

– идентификации и аутентификации персонала и пользователей по заданному перечню идентификаторов (имени, паролю, сетевому адресу и др.);

– задания и выполнения установленной в соответствии с [3] политики информационной безопасности;

– предотвращения попыток нарушения установленной политики информационной безопасности (предотвращения попыток НСД, атак из сетей общего пользования, вирусного воздействия, нарушения целостности и доступности циркулирующей информации и т. п.);

– контроля доступа к ресурсам автономных ПЭВМ, рабочих станций и серверов ЛВС на основе дискреционного принципа;

– регистрации (аудита) системных событий и событий безопасности;

– регистрации (аудита) доступа к ресурсам автономных ПЭВМ, рабочих станций и серверов ЛВС, включая попытки НСД;

– регистрации фактов отправки и получения пользователем электронных сообщений (писем, документов и др.).

**6.3.3.3** Выполнение указанных функций достигается обеспечением следующих условий:

– наличие системы идентификации и аутентификации пользователей;

– возможность управления системой безопасности (настройка прав доступа, добавление и удаление пользователей, управление паролями, управление техническими средствами (принудительное включение-выключение, изменение конфигурации) и т. п.);

– бесперебойный режим работы аппаратных и программных средств информационной системы и средств, выполняющих функции защиты, хранения, обработки и передачи защищаемой информации; возможность «зеркалирования» информации;

– регулярное резервное копирование защищаемой информации (ручное или автоматическое с возможностью настройки);

– возможность разграничения доступа пользователей к защищаемой информации и другим ресурсам информационной системы;

– реализация системы аудита действий пользователей и администратора (регистрация событий доступа пользователей к системе, регистрация событий доступа к защищаемой информации, регистрация событий безопасности); хранение журналов аудита в защищенном виде, обеспечение возможности установления ограничений на просмотр данных аудита;

– реализация системы резервного копирования защищаемой информации;

– реализация мониторинга системы администратором, оповещения администратора о событиях безопасности, удаленного управления с применением защищенных протоколов;

– резервирование критических компонентов информационной системы (линии связи, коммуникационное оборудование, серверное оборудование);

– возможность применения защищенных протоколов для доступа к информации, передачи информации в информационной системе;

– реализация системы антивирусного обеспечения (управление, обновление баз данных и т. п.);

– наличие системы тестирования при загрузке и самодиагностики в процессе работы (с генерацией сообщений нормальной работы и сообщений о сбоях, в том числе о нарушениях политики безопасности);

– возможность обнаружения угроз безопасности информационной системы (нарушения правил обработки, передачи, хранения информации, вторжений извне и т. п.).

**6.3.3.4** Система защиты должна быть защищена от несанкционированной модификации и не должна содержать пути обхода установленных механизмов контроля.

Тестирование всех функций системы защиты с помощью специальных программных средств должно проводиться администратором с установленной периодичностью.

Требования к основным компонентам системы защиты приведены в приложении Б.

### 6.3.4 Порядок применения программного и аппаратного обеспечения

**6.3.4.1** На СВТ, подключаемых к сетям общего пользования, должно быть установлено ПО только в той конфигурации, которая необходима для выполнения заявленных работ.

**6.3.4.2** Установку системного и прикладного ПО на СВТ, обеспечивающие функционирование узла доступа, должен выполнять администратор.

Установку ПО на рабочие станции пользователей должны выполнять уполномоченные специалисты под контролем администратора.

**6.3.4.3** Узел доступа размещается либо в отдельном помещении, либо в рабочем помещении администратора. Должны быть приняты организационные и технические меры по исключению несанкционированной работы в сетях общего пользования.

### 6.3.5 Общие рекомендации по размещению в государственных органах и организациях серверов общего доступа

Регистрация доменных имен в зоне .by осуществляется в соответствии с 6.1.

## 7 Требования к размещению информации на интернет-сайте. Сопровождение, продвижение и поисковая оптимизация интернет-сайта

### 7.1 Требования к размещению информации на интернет-сайте

**7.1.1** Для обеспечения актуальности размещаемой на интернет-сайте информации в государственных органах и организациях должна быть разработана и утверждена процедура эксплуатации и сопровождения интернет-сайта.

**7.1.2** Процедура должна устанавливать:

а) терминологию (для однозначного понимания положений процедуры персоналом);

б) порядок сбора сведений, подготовки информационных материалов;

в) порядок согласования, редактирования и публикации материалов на интернет-сайте;

г) порядок сопровождения интернет-сайта (планирование, модернизация, реагирование в экстренных ситуациях, регистрация и анализ нештатных ситуаций, контроль за правильностью отработки сценариев интерактивных сервисов, работоспособностью ссылок, ведением журнала сервера, посещаемостью интернет-сайта и т. д.);

д) порядок обработки запросов пользователей по электронной почте, а также запросов, поступивших при заполнении пользователями интерактивных форм;

е) ответственность на уровне структурных подразделений или отдельных сотрудников за выполнение каждой установленной функции.

***Пример – Руководитель структурного подразделения, предоставившего информацию для размещения на интернет-сайте, несет ответственность за ее содержание и достоверность, за своевременность подготовки материала к публикации, а также за соблюдение законодательства об интеллектуальной собственности;***

ж) конкретные ссылки на нормативные правовые акты (в том числе ТНПА);

з) формы документов, необходимых для осуществления процедуры.

***Примеры***

***1 Форма подачи материалов для размещения на интернет-сайте.***

***2 Форма заявки на техническое обслуживание оргтехники и т. д.***

***3 Форма квартального отчета о функционировании интернет-сайта.***

**7.1.3** Процедура эксплуатации и сопровождения интернет-сайта государственных органов и организаций должна:

– иметь статус документа, регламентирующего деятельность государственных органов и организаций, и соответствующую идентификацию;

– актуализироваться по мере необходимости;

– проходить соответствующее своему статусу согласование и утверждение в государственных органах и организациях;

– быть доступной в структурных подразделениях, на которые распространяются ее требования;

– своевременно изыматься на бумажных носителях из структурных подразделений при отмене каждой редакции.

**7.1.4** Передача функций сопровождения интернет-сайта сторонней организации допускается при наличии в этой организации системы менеджмента качества, распространяющейся на данный вид услуг.

### 7.2 Продвижение и поисковая оптимизация

При разработке интернет-сайтов необходимо учитывать, что пользователь должен легко находить интернет-сайт в сети Интернет. Для обеспечения видимости и доступности необходимо соблюдать рекомендации основных поисковых систем. Рекомендации по продвижению и поисковой оптимизации интернет-сайта приведены в приложении В.

### 7.3 Требования к системам интернет-статистики

Как минимум одна из систем интернет-статистики интернет-сайта должна основываться на данных аудита сервера, на котором размещен интернет-сайт.

Системы интернет-статистики интернет-сайтов должны:

– поддерживать основные форматы файла журнала аудита сервера (Apache Log Format, W3C Extended Log File Format, IIS Log File Format);

– иметь настройки, определяющие собственный формат файла журнала аудита;

– поддерживать анализ файлов журнала аудита сервера большого объема (превышающего 100 Мб);

– поддерживать архивный формат файлов журнала аудита сервера;

– осуществлять горячий резерв файлов журнала аудита сервера;

– анализировать наличие технических проблем (ссылки на несуществующие ресурсы, перегрузка интернет-сайта);

– генерировать отчеты статистики по обращениям программного обеспечения, посетителей и объемам информации по датам с возможностью выбора интересующего периода.

### 7.4 Требования безопасности информации для программных средств системы управления интернет-сайта

Программные средства системы управления интернет-сайта должны быть разработаны в соответствии с СТБ 34.101.37.

### 7.5 Организационные мероприятия по обеспечению безопасности информации

**7.5.1** В государственных органах и организациях назначаются лица (пользователи), допущенные к работам в сети с соответствующими полномочиями; лица, ответственные за эксплуатацию узла доступа и контроль за выполнением мероприятий по обеспечению безопасности информации при работе пользователей в сетях общего пользования (руководители подразделений и администраторы).

**7.5.2** Требования относительно обеспечения безопасности информации на СВТ, подключенных к сетям общего пользования, должны быть отражены в инструкциях администратора и пользователя, регламентирующих порядок доступа к ресурсам информационной системы, установления подлинности субъектов информационных отношений, аудита безопасности, резервирования и уничтожения информации, контроля за целостностью защищаемых сведений, защиты от вредоносного программного обеспечения и вторжений. Данные инструкции являются составной частью политики информационной безопасности, разработанной в соответствии с [3].

## Приложение А
(справочное)

## Перечень угроз безопасности интернет-сайта

**А.1** Неуполномоченное лицо (пользователь) может попытаться обойти механизмы управления доступом к активам интернет-сайта, чтобы получить доступ и использовать функции безопасности ненадлежащим образом.

**А.2** Неуполномоченное лицо может осуществлять неоднократные попытки подбора аутентификационных данных, чтобы использовать эту информацию для осуществления атак.

**А.3** Неуполномоченное лицо может осуществлять действия по подмене адреса отправителя, в результате чего информационный поток направляется в подсоединенную к серверу сеть при использовании ложного адреса отправителя.

**А.4** Неуполномоченное лицо может отправить из подсоединенной к серверу сети недозволенную информацию, что может привести к компрометации ресурсов другой подсоединенной сети.

**А.5** Неуполномоченное лицо может получить возможность просматривать, изменять и/или удалять информацию, касающуюся безопасности, которая пересылается между удаленным администратором и сервером.

**А.6** Совершаемые неуполномоченными лицами действия могут не отслеживаться, поскольку данные аудита не проверяются, что дает возможность нарушителю избежать обнаружения.

**А.7** Неуполномоченное лицо может считывать, изменять или уничтожать конфигурационные данные, критичные с точки зрения безопасности.

**А.8** Неуполномоченное лицо может вызвать потерю данных аудита или не допустить регистрации данных аудита в дальнейшем, осуществляя действия по переполнению памяти для хранения данных аудита и тем самым маскируя действия нарушителей.

**А.9** Сервер может непреднамеренно использоваться небезопасным образом неуполномоченным лицом.

**А.10** Может произойти нарушение физической целостности сервера.

**А.11** Может произойти загрузка программного обеспечения, позволяющего в дальнейшем размещать на сервере общедоступные данные.

**А.12** Администратор может умышленно не выполнять соответствующие инструкции.

**А.13** Может произойти потеря возможности управления сервером при нарушении функционирования каналов связи, по которым производится удаленное управление.

**А.14** Может произойти потеря возможности управления сервером при нарушении функционирования средств локального управления.

## Приложение Б
(справочное)

## Основные компоненты системы защиты

**Б.1** Основными компонентами системы защиты, реализуемыми программно-техническими средствами узла доступа к сетям общего пользования, являются подсистемы:

– межсетевого экранирования;
– маскирования внутреннего адресного пространства;
– обнаружения атак;
– антивирусного обеспечения;
– аудита событий безопасности, системных событий;
– аутентификации, идентификации пользователей;
– разграничения доступа.

### Б.2 Подсистема межсетевого экранирования

**Б.2.1** Подключение СВТ к сетям общего пользования проводится с обязательным применением МЭ. Подключение СВТ к сетям общего пользования в обход МЭ не допускается.

**Б.2.2** Применяемые МЭ должны иметь экспертное заключение ОАЦ на предмет реализации функций безопасности информации. Основные функциональные требования безопасности к МЭ:

а) МЭ должен соответствовать требованиям [4] по классу защищенности 3;

б) средства МЭ должны обеспечивать фильтрацию IP-пакетов на основе сетевых адресов отправителя и получателя;

в) средства МЭ должны обеспечивать фильтрацию пакетов служебного протокола ICMP (служб Ping и Traceroute);

г) средства МЭ должны обеспечивать фильтрацию с учетом значимых полей IP-протокола (длина, контрольная сумма, смещение фрагмента);

д) средства МЭ должны обеспечивать возможность блокирования IP-пакетов, использующих поле опций;

е) средства МЭ должны обеспечивать блокирование доступа в защищаемый сегмент сети по заданному списку сетевых адресов и портов IP-протокола;

ж) средства МЭ должны обеспечивать возможность динамического блокирования пользователей, со стороны которых выявлены попытки атак типов Spoofing, Address Probes, 1P Options и Port Probes, на заданный администратором период времени;

з) средства МЭ должны обеспечивать на транспортном уровне фильтрацию запросов на установление соединений со службами и сервисами стека протоколов TCP/IP;

и) МЭ должен обеспечивать на прикладном уровне защиту методом прозрачного прокси для протоколов SMTP, FTP, HTTP,DCE-RPC, H323, RealNetworks, Stream Works, VDOLive;

к) средства МЭ должны обеспечивать сокрытие сетевых адресов пользователей защищаемой сети с применением методов статического или динамического маскирования;

л) средства МЭ должны обеспечивать аутентификацию входящих соединений пользователей на основе совместной или раздельной аутентификации на сервере RADIUS, CryptoCard, SecurelD, домена Windows NT/2000 и средствами Firebox;

м) средства МЭ должны обеспечивать регистрацию событий безопасности и создание журналов на АРМ администратора безопасности или специально назначенной рабочей станции. Режимы регистрации событий, перечень регистрируемых событий должны настраиваться отдельно для каждой службы TCP/IP-протокола;

н) средства МЭ должны обеспечивать возможность подключения АРМ администратора к контроллеру средствами последовательного асинхронного интерфейса RS-232. При этом должна быть обеспечена возможность дистанционного управления МЭ и мониторинг его состояния в реальном масштабе времени;

о) средства МЭ должны обеспечивать возможность взаимодействия АРМ администратора и контроллера через ЛВС с использованием специального протокола, устойчивого к пассивным и активным методам перехвата информации. При этом должна быть обеспечена возможность дистанционного управления МЭ и мониторинг его состояния в реальном масштабе времени;

п) средства МЭ должны обеспечивать аутентификацию администратора по буквенно-цифровому паролю при его локальных и удаленных запросах на доступ;

р) программные средства МЭ должны обеспечивать установку на АРМ администратора безопасности следующих основных программных модулей:

1) утилиты инструментальной панели Control Center (менеджера системы безопасности);

2) утилиты быстрой настройки МЭ и подготовки файлов конфигурации QuickSetup Wizard;

с) утилита быстрой настройки МЭ и подготовки файлов конфигурации QuickSetup Wizard должна обеспечивать возможность подготовки и загрузки во flash-память контроллера Firebox операционной системы и файла первоначальной конфигурации, созданных в соответствии с заданными администратором безопасности установками;

т) панель SMS утилиты инструментальной панели Control Center должна обеспечивать управление конфигурацией МЭ на уровне стандартных служб TCP/IP-протокола, а также обеспечивать возможность введения уникальных и пользовательских служб;

у) средства МЭ должны обеспечивать возможность передачи уведомлений о событиях безопасности заранее заданному пользователю по каналам электронной почты. Режим передачи уведомлений должен настраиваться отдельно для каждой службы TCP/IP-протокола;

ф) средства МЭ должны обеспечивать возможность передачи сообщений о событиях безопасности заранее заданному пользователю по каналам пейджинговой связи. Режим передачи сообщений должен настраиваться отдельно для каждой службы TCP/IP-протокола с учетом направления трафика (входящая и исходящая информация);

х) средства МЭ должны обеспечивать возможность восстановления загрузочной информации и настроек параметров конфигурации после сбоев и отказов.

**Б.2.3** Доступ к ресурсам МЭ, в том числе к инструментальным средствам его конфигурирования, должен быть разрешен только назначенному администратору. Средства удаленного управления МЭ, функционирующие с использованием линий связи сетей общего пользования, должны быть исключены из конфигурации МЭ.

**Б.2.4** МЭ должен обеспечивать создание сеансов связи пользователей с внешними серверами и получать от этих серверов только ответы на запросы, сгенерированные со стороны пользователей. Настройка МЭ должна обеспечивать отказ в обслуживании любых запросов, сгенерированных извне.

**Б.2.5** МЭ должен обеспечивать реализацию функций:

– фильтрации пакетов по протоколам;

– идентификации и аутентификации пользователей;

– выполнения установленных правил политики безопасности;

– регистрации системных событий и событий безопасности;

– удаленного управления;

– оповещения администратора о попытках нарушения установленных правил политики информационной безопасности.

### Б.3 Подсистема маскирования внутреннего адресного пространства

**Б.3.1** Подсистема реализуется применением шлюзов, маршрутизаторов и т. п.

**Б.3.2** Применяемые средства маршрутизации должны иметь экспертное заключение ОАЦ на предмет реализации функций безопасности информации.

**Б.3.3** Маршрутизатор должен выполнять функции:

– маршрутизации и пакетной фильтрации сетевого трафика к сетям общего пользования;

– разделения внутреннего сетевого адресного пространства и сетей общего пользования;

– маскирования внутреннего адресного пространства (трансляции сетевых адресов).

### Б.4 Подсистема обнаружения атак

**Б.4.1** Подсистема обнаружения атак должна выполнять функции:

– обнаружения активных сетевых атак;

– автоматизированного принятия адекватных мер по обеспечению безопасности информации (уведомление администратора безопасности о нарушении установленных правил политики информационной безопасности; подача сигнала тревоги на рабочее место администратора безопасности; реализация контрмер);

– аудита (ведение журнала учета) событий безопасности;

– идентификации и аутентификации пользователей и администратора;

– удаленного управления;
– поддержки от производителя по расширению и обновлению базы сигнатур выявляемых атак;
– контроля данных аудита безопасности на МЭ, серверах и других сетевых устройствах.

**Б.4.2** Подсистема обнаружения атак должна иметь экспертное заключение ОАЦ на предмет реализации функций безопасности информации.

### Б.5 Подсистема антивирусного обеспечения

**Б.5.1** Подсистема антивирусного обеспечения должна обеспечивать:
– проверку потока данных, принимаемых и передаваемых узлом подключения к сетям общего пользования, на предмет наличия вредоносного кода;
– обнаружение и удаление вредоносного кода из потока данных;
– возможность обновления (пополнения) вирусных баз данных;
– аудит (ведение журнала учета) событий безопасности;
– оповещение администратора о попытках нарушения установленных правил политики информационной безопасности.

**Б.5.2** Подсистема антивирусного обеспечения должна иметь экспертное заключение ОАЦ на предмет реализации функций безопасности информации.

### Б.6 Подсистемы аудита событий безопасности, системных событий; аутентификации, идентификации пользователей; разграничения доступа

**Б.6.1** Функции подсистем аудита событий безопасности, системных событий; аутентификации, идентификации пользователей; разграничения доступа должны быть реализованы системным (встроенным) или прикладным ПО подсистем межсетевого экранирования, маскирования внутреннего адресного пространства, обнаружения атак.

**Б.6.2** Функции подсистемы аудита событий безопасности, системных событий реализуются встроенными средствами ОС. Основными задачами подсистемы является сбор и хранение данных аудита, предоставление администратору возможности просматривать журналы системных событий и событий безопасности с целью выявления и пресечения попыток нарушения установленных правил политики информационной безопасности.

**Б.6.3** Функции подсистемы аутентификации, идентификации пользователей реализуются средствами ОС, установленной на пользовательской ПЭВМ. Основной задачей подсистемы является проверка соответствия введенного пароля имени зарегистрированного в системе пользователя.

Функции подсистемы аутентификации, идентификации пользователей могут быть реализованы с применением специальных программно-технических средств (электронных ключей, карт и т. п.), имеющих экспертное заключение ОАЦ на предмет реализации функций безопасности информации.

**Б.6.4** Функции подсистемы разграничения доступа реализуются средствами ОС и настройкой прикладного ПО, установленных на пользовательской ПЭВМ. Основной задачей подсистемы является предоставление пользователю полномочий доступа к ресурсам пользовательской ПЭВМ и сетям общего пользования на основании предъявленного идентификатора (имени, пароля, ключа, сетевого адреса ПЭВМ и т. п.).

## Приложение В
(рекомендуемое)

## Рекомендации по продвижению и поисковой оптимизации интернет-сайта

**В.1** Доменное имя должно быть правильно подобрано: оно должно быть кратким, понятным для пользователей. URL раздела (страницы интернет-сайта) должен отражать его содержание.

**В.2** Интернет-сайт должен содержать специальную страницу, которая будет отображаться в случае перехода по ссылке на несуществующую страницу.

**В.3** На всех страницах интернет-сайта должна присутствовать служебная информация:

– тег <title> – заголовок страницы, который должен формироваться из ключевых слов страницы и быть уникальным для каждой страницы, при этом наиболее важные слова должны быть расположены ближе к началу заголовка;

– тег <description>, который выдается с результатами поиска, должен быть уникальным для каждой страницы и соответствовать содержимому страницы.

Для каждой страницы обязательно должен быть прописан язык.

**В.4** Наличие карты интернет-сайта необходимо для корректной индексации интернет-сайта поисковыми системами и обеспечения комфортной навигации.

Интернет-сайт должен содержать HTML-карту и XML-карту, сформированные на основании протокола Sitemap (http://sitemaps.org/protocol.php).

**В.5** Интернет-сайт должен содержать файл robots.txt, в котором размещается информация о пути к XML-карте, запрещенных для индексирования разделах («Результаты поиска», «Версия для печати» и др.) и т. п.

**В.6** При изменении структуры или модернизации интернет-сайта должны быть указаны переходы с основных страниц предыдущей структуры на соответствующие страницы новой структуры интернет-сайта (например, при помощи перенаправления 301 redirect, permanent redirect).

**В.7** В регламенте должна быть установлена периодичность проверки интернет-сайта на наличие неработающих ссылок (ссылки в тексте и баннеры) на несуществующие ресурсы. Такие ссылки необходимо удалять с интернет-сайта.

## Библиография

[1] Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З

[2] Приказ Оперативно-аналитического центра при Президенте Республики Беларусь «О некоторых вопросах регистрации доменных имен в пространстве иерархических имен национального сегмента сети Интернет» от 18 июня 2010 г.

[3] Постановление Совета Министров Республики Беларусь «О некоторых вопросах защиты информации» от 26 мая 2009 г. № 675

[4] Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»
Утвержден Гостехкомиссией России 25 июля 1997 г.

Ответственный за выпуск *В. Л. Гуревич*

Сдано в набор 29.01.2013. Подписано в печать 13.02.2013. Формат бумаги 60×84/8. Бумага офсетная.
Гарнитура Arial. Печать ризографическая. Усл. печ. л. 2,09 Уч.-изд. л. 1,10 Тираж 7 экз. Заказ 143

Издатель и полиграфическое исполнение:
Научно-производственное республиканское унитарное предприятие
«Белорусский государственный институт стандартизации и сертификации» (БелГИСС).
ЛИ № 02330/0552843 от 08.04.2009.
ул. Мележа, 3, комн. 406, 220113, Минск.