|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДАЮ**  Директор ООО "Активные Технологии"  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.А. Гончар  "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |  | **УТВЕРЖДАЮ**  Заказчик  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

### 

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на создание системы защиты информации

информационной системы

Версия 1.0

На листах

|  |
| --- |
| СОГЛАСОВАНО  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.В. Грецкий  "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

Минск, 2021 г.

**СОДЕРЖАНИЕ**

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 8](#_Toc76980728)

[СПИСОК СОКРАЩЕНИЙ 10](#_Toc76980729)

[1. ОБЩИЕ СВЕДЕНИЯ 10](#_Toc76980730)

[1.1. Полное наименование системы и ее условное обозначение 11](#_Toc76980731)

[1.2. Номер договора 11](#_Toc76980732)

[1.3. Наименование предприятий разработчика и заказчика системы 11](#_Toc76980733)

[1.4. Перечень документов, на основании которых создается система 11](#_Toc76980734)

[1.5. Плановые сроки начала и окончания работ по созданию системы 11](#_Toc76980735)

[1.6. Порядок оформления и предъявления заказчику результатов работ по созданию системы 12](#_Toc76980736)

[2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ 13](#_Toc76980737)

[2.1. Назначение системы 13](#_Toc76980738)

[2.2. Цели создания системы 13](#_Toc76980739)

[3. ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ 14](#_Toc76980740)

[3.1. Краткие сведения об объекте автоматизации или ссылки на документы, содержащие такую информацию 14](#_Toc76980741)

[3.2. Класс типовой информационной системы 14](#_Toc76980742)

[4. ТРЕБОВАНИЯ К СИСТЕМЕ 15](#_Toc76980743)

[4.1. Требования к структуре и функционированию 15](#_Toc76980744)

[4.1.1. Перечень систем, подсистем, их назначение и основные характеристики 15](#_Toc76980745)

[4.1.2. Требования к характеристикам взаимодействий создаваемой системы со смежными системами 16](#_Toc76980746)

[4.1.3. Требования к режимам функционирования системы 16](#_Toc76980747)

[4.1.4. Требования по диагностированию системы 16](#_Toc76980748)

[4.1.5. Перспективы развития, модернизации системы 17](#_Toc76980749)

[4.1.6. Требования к численности и квалификации персонала системы и режиму его работы 17](#_Toc76980750)

[4.1.6.1. Требования к численности персонала 17](#_Toc76980751)

[4.1.6.2. Требования к квалификации персонала 17](#_Toc76980752)

[4.1.6.3. Требуемый режим работы персонала 17](#_Toc76980753)

[4.1.7. Требования к надежности 18](#_Toc76980754)

[4.1.8. Требования к безопасности 18](#_Toc76980755)

[4.1.9. Требования к эргономике и технической эстетике 20](#_Toc76980756)

[4.1.10. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению 20](#_Toc76980757)

[4.1.11. Требования к защите информации от несанкционированного доступа 20](#_Toc76980758)

[4.1.11.1. Требование к обеспечению защиты от вредоносного программного обеспечения 20](#_Toc76980759)

[4.1.11.2. Требование к обеспечению контроля целостности 21](#_Toc76980760)

[4.1.11.3. Требование к обеспечению защиты каналов связи 21](#_Toc76980761)

[4.1.12. Требования по сохранности информации при авариях 22](#_Toc76980762)

[4.2. Требования к функциям (задачам), выполняемым системой 22](#_Toc76980763)

[4.2.1. Требования к аудиту безопасности 27](#_Toc76980764)

[4.2.1.1. Требования к определению состава информации о событиях информационной безопасности, подлежащих регистрации 27](#_Toc76980765)

[4.2.1.2. Требования к обеспечению сбора и хранения информации о событиях информационной безопасности 28](#_Toc76980766)

[4.2.1.3. Требования к централизованному сбору и хранению информации о событиях информационной безопасности 29](#_Toc76980767)

[4.2.1.4. Требования к определению способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы 30](#_Toc76980768)

[4.2.1.5. Требования к обеспечению сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации 31](#_Toc76980769)

[4.2.2. Требования по обеспечению защиты данных 31](#_Toc76980770)

[4.2.2.1. Требования к определению порядка использования съемных носителей информации, мобильных технических средств и контроля за таким использованием 31](#_Toc76980771)

[4.2.2.2. Требования по обеспечению контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации 32](#_Toc76980772)

[4.2.2.3. Требования по обеспечению защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности 32](#_Toc76980773)

[4.2.3. Требования по обеспечению идентификации и аутентификации 33](#_Toc76980774)

[4.2.3.1. Требования по разграничению доступа пользователей 33](#_Toc76980775)

[4.2.3.2. Требования по обеспечению идентификации и аутентификации пользователей 33](#_Toc76980776)

[4.2.3.3. Требования по обеспечению защиты обратной связи при вводе аутентификационной информации 34](#_Toc76980777)

[4.2.3.4. Требования по обеспечению полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей 34](#_Toc76980778)

[4.2.3.5. Требования по обеспечению контроля за соблюдением правил генерации и смены паролей пользователей 34](#_Toc76980779)

[4.2.3.6. Требования по обеспечению централизованного управления учетными записями пользователей и контроля за соблюдением правил генерации и смены паролей пользователей 35](#_Toc76980780)

[4.2.3.7. Требования по обеспечению блокировки доступа к объектам информационной системы после установленного времени бездействия (неактивности) пользователя или по его запросу 35](#_Toc76980781)

[4.2.4. Требования по защите системы защиты информации информационной системы 36](#_Toc76980782)

[4.2.4.1. Требования по обеспечению изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию 36](#_Toc76980783)

[4.2.4.2. Требования по обеспечению обновления объектов информационной системы 36](#_Toc76980784)

[4.2.4.3. Требования по обеспечению контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы 36](#_Toc76980785)

[4.2.4.4. Требования по обеспечению синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации 37](#_Toc76980786)

[4.2.5. Требования по обеспечению криптографической защиты информации 38](#_Toc76980787)

[4.2.5.1. Требования по обеспечению конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования) 38](#_Toc76980788)

[4.2.6. Требования по обеспечению защиты информации в виртуальной инфраструктуре 38](#_Toc76980789)

[4.2.6.1. Требования по обеспечению от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг 38](#_Toc76980790)

[4.2.6.2. Требования по обеспечению защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин 38](#_Toc76980791)

[4.2.6.3. Требования по обеспечению безопасного перемещения виртуальных машин и обрабатываемых на них данных 39](#_Toc76980792)

[4.2.6.4. Требования по обеспечению резервного копирования пользовательских виртуальных машин 39](#_Toc76980793)

[4.2.6.5. Требования по обеспечению резервирования сетевого оборудования по схеме N+1 40](#_Toc76980794)

[4.2.6.6. Требования по обеспечению физической изоляции сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам 40](#_Toc76980795)

[4.2.7. Иные требования 40](#_Toc76980796)

[4.2.7.1. Требования по определению перечня разрешенного программного обеспечения и регламентация порядка его установки и использования 40](#_Toc76980797)

[4.2.7.2. Требования по обеспечению контроля за составом объектов информационной системы 40](#_Toc76980798)

[4.2.7.3. Требования по автоматизированному контролю за составом средств вычислительной техники и сетевого оборудования 41](#_Toc76980799)

[4.2.7.4. Требования по использованию объектов информационной системы под пользовательскими учетными записями 41](#_Toc76980800)

[4.2.7.5. Требования по определению состава и содержания информации, подлежащей резервированию 41](#_Toc76980801)

[4.2.7.6. Требования по обеспечению резервирования информации, подлежащей резервированию 42](#_Toc76980802)

[4.2.7.7. Требования по обеспечению резервирования конфигурационных файлов сетевого оборудования 42](#_Toc76980803)

[4.2.7.8. Требования по обеспечению обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления 42](#_Toc76980804)

[4.2.7.9. Требования по обеспечению сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных 43](#_Toc76980805)

[4.2.7.10. Требования по обеспечению защиты средств вычислительной техники от вредоносных программ 43](#_Toc76980806)

[4.2.7.11. Требования по обеспечению управления внешними информационными потоками (маршрутизация) между информационными системами 44](#_Toc76980807)

[4.2.7.12. Требования по обеспечению ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями 44](#_Toc76980808)

[4.2.7.13. Требования по обеспечению ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями 45](#_Toc76980809)

[4.2.7.14. Требования по обеспечению обнаружения и предотвращения вторжений в информационной системе 46](#_Toc76980810)

[4.2.7.15. Требования по определению перечня внешних подключений к информационной системе и порядка такого подключения 46](#_Toc76980811)

[4.2.7.16. Требования по обеспечению контроля за внешними подключениями к информационной системе 47](#_Toc76980812)

[4.2.7.17. Требования к проведению внешней и внутренней проверки информационной системы 47](#_Toc76980813)

[5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗИ ИС 49](#_Toc76980814)

[6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ 49](#_Toc76980815)

[6.1. Виды испытаний системы 50](#_Toc76980816)

[6.1.1. Состав, объем и методы испытаний системы 50](#_Toc76980817)

[6.1.2. Опытная эксплуатация системы 50](#_Toc76980818)

[6.1.3. Приемочные испытания системы 50](#_Toc76980819)

[6.1.4. Аттестация системы защиты информации 51](#_Toc76980820)

[6.2. Общие требования к приемке работ по стадиям 52](#_Toc76980821)

[6.2.1. Перечень участвующих предприятий и организаций 52](#_Toc76980822)

[6.2.2. Место и сроки проведения испытаний 53](#_Toc76980823)

[6.2.3. Порядок согласования и утверждения приемочной документации 53](#_Toc76980824)

[7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ 54](#_Toc76980825)

[Приложение 1 55](#_Toc76980826)

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем ТЗ применяют следующие термины с соответствующими определениями, приведенными в СТБ 34.101.1-2014 со следующими дополнениями:

**автоматизированная информационная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

**аутентификация участника** – подтверждение достоверности сведений объекта, полученных в ходе его идентификации;

**идентификация** - это определение пользователя в автоматизированной системе (например, в интернет-банке) по уникальному признаку – идентификатору.

**доступность** – свойство, характеризующее возможности ИС предоставлять необходимые ресурсы (вычислительные, коммуникационные, информационные, функциональные) авторизованным субъектам (пользователям, процессам) в требуемое им время;

**защита информации** – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности (неизменности), подлинности, доступности и сохранности информации;

**информационная безопасность** – состояние информационной системы, при котором с требуемой вероятностью обеспечиваются конфиденциальность, целостность, подлинность, доступность и сохранность защищаемой информации;

**информационная система** – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

**конфиденциальность информации** – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;

**персональные данные** – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано на основании такой информации;

**подлинность** – свойство информации, гарантирующее, что информация идентична оригинальной (заявленной).

**сохранность** – свойство информации, гарантирующее, что информация ни при каких условиях не может быть уничтожена (удалена).

**физическое лицо, которое может быть идентифицировано** – физическое лицо, которое может быть прямо или косвенно определено, в частности через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

**целостность –** свойство информации сохранять свое информационное содержание и однозначность интерпретации в условиях случайных или преднамеренных воздействий;

**центр обработки данных** – комплекс вычислительных и программных систем, систем хранения данных, расположенных в отдельном специализированном помещении или здании, подключенный высокоскоростными каналами связи к опорной сети передачи данных.

# СПИСОК СОКРАЩЕНИЙ

|  |  |
| --- | --- |
| **ГОСТ** | Государственный стандарт |
| **ИС** | Информационная система |
| **ИТ** | Информационные технологии |
| **ЛНПА** | Локальные нормативно-правовые акты |
| **НСД** | Несанкционированный доступ |
| **ОС** | Операционная система |
| **ПО** | Программное обеспечение |
| **РД** | Руководящий документ |
| **СЗИ** | Система защиты информации |
| **СКЗИ** | Средства криптографической защиты информации |
| **СТБ** | Стандарты Республики Беларусь |
| **ТЗ** | Техническое задание |
| **ТР** | Технический регламент |
| **ЦОД** | Центр обработки данных |
| **IP-адрес** | Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP (Internet Protocol Address) |
| **MAC-адрес** | Уникальный идентификатор, присваиваемый каждой единице активного оборудования ( Media Access Control) |
| **TCP** | Протокол управления передачей (Transmission Control Protocol) |
| **VPN** | Виртуальная частная сеть (Virtual Private Network) |

# ОБЩИЕ СВЕДЕНИЯ

Настоящее техническое задание (далее – ТЗ) является основным документом, определяющим требования и порядок создания системы защиты информации (далее – СЗИ) ИС в соответствии с которым приводится ее разработка и приемка при вводе в действие.

## 1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: ИС.

Условное обозначение системы: СЗИ ИС.

## 1.2. Номер договора

Настоящее ТЗ разработано на основании договора возмездного оказания услуг № 5 от 04.05. 2020 г.

## 1.3. Наименование предприятий разработчика и заказчика системы

Заказчик: ЗАО «Специальная финансовая организация «Центр секьюритизации»» (далее – Заказчик).

Юридический адрес: г. Минск, ул. Освобождения, дом 3, помещение 2.

Исполнитель: ООО "Активные технологии" (далее – Исполнитель).

Юридический адрес: Республика Беларусь, 220005, г. Минск, ул Притыцкого, д. 156, этаж 15.

## 1.4. Перечень документов, на основании которых создается система

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 "О совершенствовании государственного регулирования в области защиты информации".

Постановление Совета министров Республики Беларусь от 1 марта 2019 г. № 139 "О мерах по реализации Указа Президента Республики Беларусь" от 7 августа 2018 г. № 305.

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации".

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 "О мерах по реализации Указа Президента Республики Беларусь" от 9 декабря 2019 г. № 449.

Выполнение перечисленных выше этапов работ по созданию СЗИ ИС осуществляется в рамках следующих лицензий Исполнителя:

Специальное разрешение (лицензия) № 01019/146 на право осуществления деятельности по технической и (или) криптографической защите информации от 23.12.2020 г.

## 1.5. Плановые сроки начала и окончания работ по созданию системы

Сроки проведения работ по созданию СЗИ ИС определяется в соответствии с договором возмездного оказания услуг № 5 от 04.05.2020 г.

## 1.6. Порядок оформления и предъявления заказчику результатов работ по созданию системы

Документация, предъявляемая Заказчику, должна быть разработана и оформлена в соответствии с требованиями следующих документов:

* Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь 20.02.2020 № 66;
* ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы";
* РД 50-34.698-90 "Методические указания. Информационная технология. Комплекс Стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов".

Документы, являющиеся результатом работ, предоставляются Исполнителем Заказчику в 2-х экземплярах на бумажных носителях и в 1-м экземпляре в электронном виде.

Документы в электронном виде предоставляются в формате PDF посредством электронной почты.

# НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

## 2.1. Назначение системы

Назначением СЗИ ИС является снижение вероятности реализации угроз нарушения конфиденциальности, целостности, подлинности, доступности и сохранности в отношении информации, распространение и (или) предоставление которой ограничено, не отнесенных к государственным секретам, обрабатываемых в ИС.

СЗИ ИС предназначена для:

* проведения аудита событий информационной безопасности;
* обеспечения защиты данных;
* обеспечения идентификации и аутентификации;
* защиты системы защиты информации информационной системы;
* обеспечения криптографической защиты информации;
* защиты виртуальной инфраструктуры;
* защиты от вредоносного программного обеспечения;
* предотвращения вторжения в информационную систему;
* защиты от отказа в обслуживании.

Кроме того, СЗИ ИС предназначена для автоматизации процесса управления информационной безопасностью ИС.

## 2.2. Цели создания системы

Целями создания СЗИ ИС являются:

* обеспечение конфиденциальности, целостности, подлинности, доступности, и сохранности информации, предоставление и (или) распространение которой ограничено, не отнесенной к государственным секретам;
* соответствие требованиям законодательства Республики Беларусь в части защиты информации;

# ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ

## 3.1. Краткие сведения об объекте автоматизации или ссылки на документы, содержащие такую информацию

Заказчиком на проведение работ по созданию СЗИ ИС является ЗАО «Специальная финансовая организация «Центр секьюритизации»». Основной вид деятельности Заказчика – финансирование специальной финансовой организацией инициатора (инициаторов) под уступку прав (требований) за счет средств, привлеченных путем эмиссии облигаций, либо с последующей эмиссией облигаций

Администрирование ИС производится в соответствии с руководством администратора ИС.

Пользователями ИС являются граждане Республики Беларусь, прошедшие регистрацию и идентификацию в ИС.

## 3.2. Класс типовой информационной системы

Обрабатываемая в ИС информация, а именно: фамилия, собственное имя, дата рождения, пол, номер паспорта, классифицируется как персональные данные в соответствии с положениями Закона Республики Беларусь от 21 июля 2008 г. №418-З "О регистре населения” и Закона Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации".

В соответствии с СТБ 34.101.30-2017 "Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация" ИС отнесена к классу **3-фл**, **3-юл**, на основании типов обрабатываемой информации, информационных потоков.

# ТРЕБОВАНИЯ К СИСТЕМЕ

Совокупность программных, технических, программно-технических СЗИ ИС и поддерживающие их организационные меры должны обеспечивать защиту данных, обрабатываемых в ИС, от угроз безопасности.

СЗИ ИС должна обеспечивать выполнение требований Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

## 4.1. Требования к структуре и функционированию

Структура ИС должна включать подсистемы защиты информации, определяемые требованиями нормативных документов, указанных в п. 1.4. настоящего ТЗ.

Функции подсистемы защиты информации СЗИ ИС должны быть направлены на защиту данных, обрабатываемых в ИС.

Требования к серверному оборудованию для установки ПО СЗИ ИС определяется разработчиком ПО ИС и минимально должно соответствовать требованиям, указанным в таблице 1.

Таблица 1 – Требования к серверному оборудованию

|  |  |  |
| --- | --- | --- |
| **Назанчение** | **Сервер** | **Спецификация** |
| VM1 | Ubuntu Server 16.04.6 | 4CPU 2300GHZ  4GB RAM  HDD 250GB |
| VM2 | Ubuntu Server 16.04.6 | CPU 2300GHZ  1GB RAM  HDD 30GB |
| VM3 | Debian 6.08 | CPU 2300GHZ  1GB RAM  HDD 8GB |

### 4.1.1. Перечень систем, подсистем, их назначение и основные характеристики

СЗИ ИС должна состоять из следующих подсистем:

* проведения аудита событий информационной безопасности;
* обеспечения защиты данных;
* обеспечения идентификации и аутентификации;
* защиты системы защиты информации информационной системы;
* обеспечения криптографической защиты информации;
* защиты виртуальной инфраструктуры;
* защиты от вредоносного программного обеспечения;
* предотвращения вторжения в информационную систему;
* защиту от отказа в обслуживании.

## 4.1.2. Требования к характеристикам взаимодействий создаваемой системы со смежными системами

ИС должна взаимодействовать со следующими смежными системами по защищенным каналам передачи данных организованным с использованием средств криптографической защиты информации, имеющих сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY):

* ИС Банковско-финансовой телесети;
* ИС «Белгазпромбанка»
* Иные системы контрагентов в рамках перспективного развития ИС Заказчика.

## 4.1.3. Требования к режимам функционирования системы

Режим функционирования СЗИ ИС – круглосуточный (24 часа в день и 7 дней в неделю), исключая согласованные периоды времени на выполнение регламентных работ по обслуживанию оборудования или обновление программного обеспечения СЗИ ИС.

Для СЗИ ИС предусмотрены следующие режимы работы:

1. Штатный режим – весь функционал СЗИ ИС работает в соответствии с возложенными на него функциями;
2. Аварийный режим – функционал СЗИ ИС не работает в соответствии с возложенными на него функциями или полностью не работает;
3. Режим сервисного обслуживания – функционал СЗИ ИС работает в соответствии с возложенными на него функциями, но некоторые функции могут быть временно отключены или перестроены администраторами СЗИ ИС.

СЗИ ИС должна функционировать в штатном режиме работы непрерывно и круглосуточно.

## 4.1.4. Требования по диагностированию системы

Диагностирование СЗИ ИС должно осуществляться на периодической основе в процессе ее эксплуатации. По результатам работы данного функционала пользователю СЗИ ИС должны выводиться следующие сообщения:

* об окончании самодиагностики и нормальной работе СЗИ ИС;
* о наличии проблем в работе СЗИ ИС.

СЗИ ИС должна удовлетворять следующим требованиям по диагностированию:

* регистрацию системных ошибок в ходе выполнения работы в системном журнале;
* журналирование действий пользователей при выполнении работ;
* выдача пользователю сообщений, содержащих адекватное описание нарушений работоспособности СЗИ ИС.

## 4.1.5. Перспективы развития, модернизации системы

СЗИ ИС должна создаваться с учетом возможностей ее расширения при увеличении числа одновременно подключенных пользователей, серверов и активного сетевого оборудования СЗИ ИС.

## 4.1.6. Требования к численности и квалификации персонала системы и режиму его работы

### 4.1.6.1. Требования к численности персонала

С учетом масштабируемости ИС конкретных требований к численности пользователей не приводится и определяются разработчиками ИС.

В ИС предполагается наличие следующих ролей пользователей:

* внешний пользователь;
* администратор ИС;

### 4.1.6.2. Требования к квалификации персонала

Персонал, работающий с ИС должен быть ознакомлен с политиками информационной безопасности Заказчика.

### 4.1.6.3. Требуемый режим работы персонала

Режим работы персонала, задействованного в администрировании СЗИ ИС, определяется режимом работы Заказчика, эксплуатирующей СЗИ ИС, за исключением работ по устранению возможных ошибок ПО, а также при переходе СЗИ ИС в аварийный режим или режим сервисного обслуживания.

## 4.1.7. Требования к надежности

Надежность и оперативная готовность СЗИ ИС должна обеспечиваться выполнением следующих требований:

* возможность непрерывной работы с учетом перерывов, необходимых для сервисного обслуживания;
* оперативное восстановление данных и работоспособности оборудования СЗИ ИС в случаях вывода из строя оборудования и при чрезвычайных ситуациях.

Надежное (устойчивое) функционирование СЗИ ИС должно обеспечиваться выполнением совокупности организационно-технических мероприятий:

* организацией бесперебойного питания технических средств;
* организацией своевременного технического обслуживания;
* необходимым уровнем квалификации сотрудников профильных подразделений.

В целях обеспечения надежности поддержки точного времени событий должен использоваться сервер получения точного времени и трансляция эталонного значения времени на серверы и сетевое оборудование СЗИ ИС. Источником сигналов точного времени (синхронизации) должен являться сервер точного времени Национального эталона времени и частоты Республики Беларусь, который позволяет синхронизировать время компьютера в соответствии со шкалой времени Национального эталона времени и частоты Республики Беларусь БелГИМ.

## 4.1.8. Требования к безопасности

Для реализации задач безопасности должны использоваться комплексные меры по защите информации:

правовые – заключение со сторонними организациями соглашений, в которых устанавливаются условия пользования информацией, а также ответственность сторон по таким соглашениям за нарушение указанных условий;

организационные – обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к аппаратному и программному обеспечению, информации (материальным носителям информации), а также разграничение доступа к информации по уровню доступа пользователей и категории информации;

технические – использование средств технической и криптографической защиты информации, имеющих сертификаты соответствия ТР 2013/027/BY, выданные в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь, а также меры по контролю защищенности информации.

В качестве источников угроз СЗИ ИС должны рассматриваться следующие классы источников:

* + пользователи ИС, которые могут ошибочно получить доступ к активам ИС в нарушение установленных политик безопасности, используя оплошности и ошибки со стороны администраторов СЗИ ИС или других авторизованных пользователей, недостатки (слабые места) средств безопасности;
  + администраторы СЗИ ИС, которые могут допускать ошибки при управлении ресурсами, активами и средствами безопасности СЗИ ИС;
  + внешние субъекты (нарушители), которые могут пытаться из любопытства или со злонамеренными целями осуществить перехват данных, передаваемых по каналам связи, а также предпринимать технические атаки с целью получения доступа к активам ИС или нарушения ее доступности;
  + мошенники (нарушители), которые могут действовать с применением программного обеспечения и (или) технических устройств, оказывающих воздействие на функционирование информационной системы;
  + сбои и отказы оборудования, программные сбои, которые могут привести к нарушению безопасного состояния активов ИС;
  + вредоносные программные коды (вирусы), которые могут повлиять на нарушение целостности или доступности данных.

СЗИ ИС обеспечивать защиту:

– данных безопасности СЗИ ИС (конфигурация СЗИ ИС, данные аудита, данные идентификации и аутентификации и т.д.);

– данных СЗИ ИС, обрабатываемых и создаваемых в результате автоматизированных процессов;

– прикладного программного обеспечения, обеспечивающего реализацию автоматизированных процессов деятельности СЗИ ИС.

Основные активы, ресурсы и оборудование СЗИ ИС должны располагаться в зоне контроля физического доступа.

Специальных требований к безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств СЗИ Платформы ИС не предъявляется. Сотрудники Заказчика и Исполнителя должны руководствоваться действующими в Организации регламентирующими технику безопасности документами.

## 4.1.9. Требования к эргономике и технической эстетике

Ввиду того, что для доступа к СЗИ ИС пользователь может выбрать любой браузер, удовлетворяющий требованиям программного обеспечения, изложенным в настоящем ТЗ, требования к пользовательскому интерфейсу не предъявляются и определяются разработчиком ИС.

## 4.1.10. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению

Функции СЗИ ИС должны предоставляться в круглосуточном бесперебойном режиме. Регламентные работы по обслуживанию оборудования и программного обеспечения должны выполняться обслуживающим персоналом согласно договора, заключенного с обслуживающей организацией.

При проведении регламентных в рабочее время пользователи ИС должны быть предупреждены путем уведомления с указанием факта проведения регламентных работ.

В СЗИ ИС должна быть обеспечена возможность, в случае отказа оборудования или программного обеспечения, осуществить восстановление ее функционирования из резервной копии.

## 4.1.11. Требования к защите информации от несанкционированного доступа

### 4.1.11.1. Требование к обеспечению защиты от вредоносного программного обеспечения

Антивирусное программное обеспечение предназначено для защиты от воздействия вредоносного программного кода информационных объектов физического оборудования (серверов и рабочих станций) и виртуальной среды в которой размещается ИС.

Антивирусное программное, при наличии технической возможности, обеспечение должно быть установлено на всех рабочих станциях работников Заказчика, а также на серверах ИС.

Антивирусное программное обеспечение должно иметь возможность централизованного управления, обновления самого антивирусного программного обеспечения и обновления сигнатур вредоносных программ.

Антивирусное программное обеспечение должно иметь функцию самодиагностики. При возникновении сбоя или отключения защиты от вредоносного программного обеспечений, антивирусное программное обеспечение должно оповестить пользователя посредством всплывающего окна и администратора в консоли администрирования либо другим доступным способом.

Антивирусное программное обеспечение должно поддерживать возможность определения вредоносного программного обеспечения, не входящего в сигнатуры (эврестический анализ) в режиме реального времени.

Защита от вредоносного программного обеспечения должна осуществляться с применением лицензионного антивирусного программного обеспечения, имеющего сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY).

### 4.1.11.2. Требование к обеспечению контроля целостности

В ИС должно применяться средство контроля целостности, позволяющее контролировать:

* исполняемые файлы;
* файлы конфигурации.

Применяемое средство контроля целостности исполняемых файлов и конфигурации СЗИ ИС должно выполнять следующие операции:

* вычисление значения функции хэширования данных согласно заданному алгоритму;
* проверку целостности данных по вычисленным ранее хэш-значениям согласно заданному алгоритму;
* проверку работоспособности, включая средства самотестирования и контроля целостности.

Функция контроля целостности исполняемых файлов и файлов конфигурации СЗИ ИС должна осуществляться с применением программного обеспечения, имеющего сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY).

### 4.1.11.3. Требование к обеспечению защиты каналов связи

Для удаленного администрирования должны использоваться каналы связи, защищенные с применением криптографических средств, обеспечивающие надежную аутентификацию сторон, участвующих в обмене данными, и шифрование их сетевого трафика путем организации VPN канала передачи данных.

Сеть для администрирования ИС должна быть логически изолирована от сети передачи данных.

Удаленный доступ к ИС для администрирования должен осуществляться по защищенному каналу связи, организованному с использованием средств криптографической защиты информации, имеющих сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY).

### 4.1.12. Требования по сохранности информации при авариях

При создании СЗИ ИС должно использоваться аппаратное и (или) программное обеспечение для резервирования и создания резервных копий данных ИС.

При авариях не должна нарушаться целостность информации.

Требования надежности системы в целом и сохранности информации во время аварий должны быть учтены при выборе аппаратного и (или) программного обеспечения и квалификации обслуживающего персонала.

## 4.2. Требования к функциям (задачам), выполняемым системой

В таблице 4.2 приведен перечень требований к СЗИ ИС согласно Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

Таблица 4.2 – Перечень требований к СЗИ ИС

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Наименование требования** | **Условие об обязательности выполнения требований в соответствии с классом** | |
| **3-фл** | **3-юл** |
| **1.** | **Аудит безопасности** |  |  |
| 1.1. | Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое) | + | + |
| 1.2. | Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года | + | + |
| 1.3. | Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года | +/– | +/– |
| 1.4. | Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы | + | + |
| 1.5 | Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года | + | + |
| **2.** | **Требования по обеспечению защиты данных** |  |  |
| 2.1. | Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием | + | + |
| 2.2. | Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации | + | + |
| 2.3. | Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности | + | + |
| **3.** | **Требования по обеспечению идентификации и аутентификации** |  |  |
| 3.1. | Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации | + | + |
| 3.2. | Обеспечение идентификации и аутентификации пользователей информационной системы | + | + |
| 3.3. | Обеспечение защиты обратной связи при вводе аутентификационной информации | + | + |
| 3.4. | Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы | + | + |
| 3.5. | Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы | + | + |
| 3.6. | Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы | +/– | + |
| 3.7. | Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу | + | + |
| **4.** | **Требования по защите системы защиты информации информационной системы** |  |  |
| 4.1. | Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию | + | + |
| 4.2. | Обеспечение обновления объектов информационной системы | + | + |
| 4.3. | Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы | + | + |
| 4.4. | Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации | + | + |
| **5.** | **Обеспечение криптографической защиты информации** |  |  |
| 5.1. | Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования) | + | + |
| 5.2. | Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования) | +/– | +/– |
| 5.3. | Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи) | + | + |
| 5.4. | Обеспечение контроля целостности данных в информационной системе (средства контроля целостности) | +/– | +/– |
| 5.5. | Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены) | +/– | +/– |
| 5.6. | Обеспечение идентификации и аутентификации в информационной системе (криптографические токены) | +/– | +/– |
| **6.** | **Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре** |  |  |
| 6.1. | Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг | + | + |
| 6.2. | Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин | + | + |
| 6.3. | Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных | + | + |
| 6.4. | Обеспечение резервного копирования пользовательских виртуальных машин | + | + |
| 6.5. | Обеспечение резервирования сетевого оборудования по схеме N+1 | + | + |
| 6.6. | Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам | +/– | + |
| **7.** | **Иные требования** |  |  |
| 7.1. | Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования | + | + |
| 7.2. | Обеспечение контроля за составом объектов информационной системы | + | + |
| 7.3. | Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования | +/– | + |
| 7.4. | Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы) | + | + |
| 7.5. | Определение состава и содержания информации, подлежащей резервированию | + | + |
| 7.6. | Обеспечение резервирования информации, подлежащей резервированию | + | + |
| 7.7. | Обеспечение резервирования конфигурационных файлов сетевого оборудования | + | + |
| 7.8. | Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления | + | + |
| 7.9. | Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных | +/– | + |
| 7.10. | Обеспечение защиты средств вычислительной техники от вредоносных программ | + | + |
| 7.11. | Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ | +/– | + |
| 7.12. | Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ | + | + |
| 7.13. | Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего) | + | + |
| 7.14. | Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях | + | + |
| 7.15. | Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях | +/– | +/– |
| 7.16. | Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений | + | + |
| 7.17. | Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений | + | + |
| 7.18. | Обеспечение обнаружения и предотвращения утечек информации из информационной системы. Использование системы обнаружения и предотвращения утечек информации из информационной системы | +/– | +/– |
| 7.19. | Определение перечня внешних подключений к информационной системе и порядка такого подключения | + | + |
| 7.20. | Обеспечение контроля за внешними подключениями к информационной системе | + | + |
| 7.21. | Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы | +/– | +/– |

### 4.2.1. Требования к аудиту безопасности

#### 4.2.1.1. Требования к определению состава информации о событиях информационной безопасности, подлежащих регистрации

Средства аудита СЗИ ИС должны обеспечивать:

* регистрацию событий, связанных с действиями пользователей системы над объектами ИС;
* событий удачных/неудачных входов пользователя в систему;
* событий создания, изменения прав, удаления пользователей.

Все события безопасности должны содержать информацию о времени и дате события, идентификаторе пользователя, иденцифицировавшего событие, тип события (описание события).

Для тех событий аудита, которые связаны с действиями идентифицированных пользователей, всякое подлежащее аудиту событие должно быть связано с идентификатором пользователя, вызвавшего это событие.

#### 4.2.1.2. Требования к обеспечению сбора и хранения информации о событиях информационной безопасности

Подсистема аудита безопасности должна обеспечивать:

* сбор и хранение информации о событиях информационной безопасности, подлежащих регистрации ИС;
* предоставление доступа уполномоченным администраторам к хранимым событиям информационной безопасности, а также предоставление возможности определения способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченным на это пользователям информационной системы;
* сбор и хранение информации о функционировании средств вычислительной техники, сетевого оборудования и СЗИ;
* контроль за функционированием подсистемы аудита безопасности.

В СЗИ ИС должно производиться определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

События безопасности должны содержать следующие сведения:

* идентификаторы (столько, сколько доступно) для субъекта, запрашивающего действие (например, идентификатор пользователя, имя компьютера, IP-адрес и MAC-адрес);
* идентификаторы (столько, сколько доступно) для объекта, в отношении которого было выполнено действие (например, имена файлов, к которым был получен доступ, уникальные идентификаторы записей, к которым был получен доступ в базе данных, IP-адрес и MAC-адрес);
* дата и время;
* активность события (например, вход в систему и выход из нее);
* изменения прав пользователя;
* изменение параметров системы;
* статус деятельности по обеспечению безопасности (например, успех или неудача, отказ или разрешение).
* тип доступа (например, чтение, запись, исполнение).
* сигналы тревоги, подаваемые системами контроля доступа и сетевого мониторинга.

К срокам хранения событий информационной безопасности предъявляются следующие требования:

* хранение информации о событиях информационной безопасности, подлежащих регистрации СЗИ ИС собранных событий информационной безопасности не менее 1 (одного) года;
* хранение информации о функционировании средств вычислительной техники, сетевого оборудования и СЗИ не менее 1 (одного) года;

Все записи аудита должны быть защищены от модификации и удаления. При превышении установленного порогового значения журнала данных аудита подсистема хранения данных аудита должна предпринять действия по сохранению журнала аудита в файле. Количество сохраненных файлов аудита должно быть ограничено. Если количество сохранённых файлов аудита превышает установленное значение, данные аудита записываются вместо самых ранних файлов, которые в свою очередь должны передаваться в архив.

#### 4.2.1.3. Требования к централизованному сбору и хранению информации о событиях информационной безопасности

В ИС должны осуществляться централизованный сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

* возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени;
* генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);
* хранение информации о событиях безопасности в течение установленного времени;

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

Правила и процедуры сбора, записи и хранения информации о событиях безопасности должны быть регламентированы.

#### 4.2.1.4. Требования к определению способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы

Уполномоченные администраторы должны иметь возможность чтения всей информации о событиях из записей данных аудита СЗИ ИС.

Записи аудита должны предоставляться в таком виде, чтобы пользователю было удобно интерпретировать информацию.

Доступ к чтению записей аудита должен быть разрешен только для тех пользователей, которым доступ к чтению точно предоставлен.

Возможность выполнения поиска и сортировки данных аудита должна предоставляться на основе:

* операции;
* даты события;
* времени события;
* идентификатора объекта;
* идентификатора субъекта.

Уполномоченный сотрудник Организации должен осуществлять мониторинг событий информационной безопасности, связанный со:

* сбоями в механизмах сбора информации;
* достижением установленного порогового значения журнала данных аудита.

Периодичность мониторинга (просмотра, анализа) журналов событий информационной безопасности должна быть определена Заказчиком в политике контроля (мониторинга) над функционированием ИС.

#### 4.2.1.5. Требования к обеспечению сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации

В СЗИ ИС должен быть реализован сбор информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации.

Перечень средств вычислительной техники, сетевого оборудования и средств защиты информации представлен в таблице 4.2.1.

Таблица 4.2.1 –

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Наименование оборудование** | **Срок хранения информации** |
|  |  |  |
|  |  |  |

К срокам хранения событий информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации предъявляются следующие требования:

* хранение информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации СЗИ ИС не менее 1 (одного) года.

### 4.2.2. Требования по обеспечению защиты данных

#### 4.2.2.1. Требования к определению порядка использования съемных носителей информации, мобильных технических средств и контроля за таким использованием

В качестве мобильных технических средств рассматриваются съемные машинные носители персональных данных (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки персональных данных (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

Все используемые носители информации должны эксплуатироваться с соблюдением требований и правил безопасности, установленных в организации, эксплуатирующей ИС.

Заказчик должен принимать организационно-технические меры по выявлению, анализу и блокированию в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации. Использование мобильных и других беспроводных устройств должно быть строго регламентировано.

В СЗИ ИС должна быть предусмотрена возможность использования съемных носителей информации. Требования к порядку использования съемных носителей информации должны соответствовать Политике использования съемных носителей информации Заказчика.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание, должны регламентироваться в Политике использования съемных носителей информации Заказчика.

#### 4.2.2.2. Требования по обеспечению контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации

В СЗИ ИС должен осуществляться контроль правильности установленных параметров используемых политик безопасности, приложений и служб, значения настроек в файлах конфигурации системы, обновлений сигнатурных баз средств защиты, а также контроль неизменности настроек файлов конфигурации программного обеспечения СЗИ ИС (включая настройки виртуальной инфраструктуры) и средств безопасности.

Контроль конфигураций системы должен обеспечиваться с целью мониторинга и анализа параметров настройки ПО и СЗИ ИС.

Должен обеспечиваться контроль за установкой обновлений программного обеспечения, средств защиты информации (сигнатур антивирусных средств и средств обнаружения вторжений).

Должен обеспечиваться контроль за использованием в СЗИ ИС только разрешенного ПО.

#### 4.2.2.3. Требования по обеспечению защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности

В СЗИ ИС должны быть реализованы механизмы защиты хранящихся записей аудита, резервных копий, параметров настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности от неавторизованного удаления. СЗИ ИС должны предотвратить неавторизованное изменение этих данных.

Для реализации механизмов СЗИ ИС должна проводить идентификацию и аутентификацию пользователей прежде, чем им будет разрешено предпринять какие-либо действия. Кроме того, в СЗИ ИС должна применяться ролевая модель разграничения прав пользователей, позволяющая разграничить права пользователей между объектами ИС.

### 4.2.3. Требования по обеспечению идентификации и аутентификации

#### 4.2.3.1. Требования по разграничению доступа пользователей

Для доступа к СЗИ ИС должна использоваться ролевая политика управления доступа.

В СЗИ ИС должен предоставляться доступ зарегистрированным пользователям СЗИ ИС только к тем ресурсам, операциям и данным, для которых они авторизованы в соответствии с назначенными правами доступа на основе атрибутов безопасности.

Пользователи СЗИ ИС должны иметь следующие роли:

* администратор СЗИ ИС;

#### 4.2.3.2. Требования по обеспечению идентификации и аутентификации пользователей

В зависимости от категории пользователей СЗИ ИС для входа в систему должны использоваться различные механизмы идентификации и аутентификации.

Доступ ко всем ресурсам и данным ИС до проведения успешной идентификации и аутентификации должен быть закрыт.

Все пользователи ИС должны быть зарегистрированы в системе путем задания атрибутов учетной записи. Только авторизованные пользователи могут получать доступ к активам ИС.

В СЗИ ИС должны быть предусмотрены следующие категории пользователей:

* администратор СЗИ ИС;

Для получения доступа к системе пользователь должен быть зарегистрирован и идентифицирован.

В процессе прохождения процедуры идентификации и аутентификации пользователь должен вводить значение идентификатора и пароля учетной записи. В процессе ввода пароля символы пароля должны отображаться в маскирующем виде.

Если зарегистрированным пользователем многократно (установленное уполномоченным администратором число, но не более десяти раз) вводится неправильный пароль, то учётная запись пользователя должна автоматически блокироваться на один час. Значение количества попыток ввода пароля устанавливается администратором в процессе настройки политики блокировки учетной записи.

При использовании Active Directory политика пароля, определяющая сложность пароля устанавливается при настройке каталога Active Directory.

#### 4.2.3.3. Требования по обеспечению защиты обратной связи при вводе аутентификационной информации

В процессе аутентификации пользователю СЗИ ИС должны отображаться только маскирующие символы пароля.

Не допускается отображения вводимых символов в полях, предназначенных для ввода паролей.

#### 4.2.3.4. Требования по обеспечению полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей

Доступ к ресурсам и данным ИС в процессе обработки, передачи и хранения должен предоставляться на основе атрибутов объектов и пользователей и строго контролироваться.

В ИС должны поддерживаться административные и пользовательские роли для разделения доступа к объектам и функциям ИС.

Функции по управлению конфигурационными данными ресурсов ИС, атрибутами безопасности и данными должны предоставляться только уполномоченным администраторам ИС.

В ИС должен предоставляться доступ зарегистрированным пользователям ИС только к тем ресурсам, операциям и данным, для которых они авторизованы в соответствии с назначенными правами доступа на основе атрибутов безопасности.

Для каждого пользователя должен поддерживаться следующий список атрибутов безопасности:

* имя пользователя;
* роль;
* пароль.

В СЗИ ИС должна быть реализована политика управления доступом к настройкам средств безопасности, предусматривающую возможность создания, чтения, модификации, над атрибутами безопасности только уполномоченному администратору.

#### 4.2.3.5. Требования по обеспечению контроля за соблюдением правил генерации и смены паролей пользователей

В СЗИ ИС должны обеспечивать механизм для верификации того, что секреты удовлетворяют следующим требованиям:

* длина не менее 8 символов;
* в пароле должны встречаться минимум одна цифра, одна заглавная буква латинского алфавита, одна прописная буква латинского алфавита и один специальный символ (! @ # $ % ^ & \* ( ) / \ \_ = + - ?).

Требования к паролям пользователей устанавливаются на основании соответствующей политики парольной защиты.

Установка и изменение пароля должно контролироваться парольной политикой, которая устанавливает ограничения на минимальную длину пароля и использование в пароле различных символов. Устанавливать новые значения параметров парольной политики вместо заданных по умолчанию могут только соответствующие уполномоченные администраторы.

#### 4.2.3.6. Требования по обеспечению централизованного управления учетными записями пользователей и контроля за соблюдением правил генерации и смены паролей пользователей

В ИС должны поддерживаться административные и пользовательские роли для разделения доступа к объектам и функциям ИС.

Все учетные записи пользователей, являющихся работниками Заказчика, должны быть зарегистрированы в каталоге Active Directory.

При управлении учетными записями пользователей ИС должны быть реализованы механизмы централизованного управления. Доступ к данным учетных записей пользователей должен предоставляться только уполномоченному администратору.

Требования по управлению учетными записями пользователей ИС должны соответствовать политике управления учетными записями пользователей Заказчика.

Требования по правилам генерации и смены паролей пользователей в СЗИ ИС должны соответствовать политике создания, защиты и хранения паролей Заказчика.

#### 4.2.3.7. Требования по обеспечению блокировки доступа к объектам информационной системы после установленного времени бездействия (неактивности) пользователя или по его запросу

В СЗИ ИС должны быть реализованы следующие возможности:

* возможность авторизованному пользователю завершить свой интерактивный сеанс связи;
* возможность завершения интерактивного сеанса связи авторизованного пользователя после настраиваемого времени его бездействия (по умолчанию не менее тридцати минут). Данная функция безопасности предотвращает несанкционированный физический доступ к ресурсам рабочего стола пользователя, оставленного без присмотра.

### 4.2.4. Требования по защите системы защиты информации информационной системы

#### 4.2.4.1. Требования по обеспечению изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию

В СЗИ ИС должна быть реализована возможность осуществлять ролевую политику управления доступом, чтобы обеспечить ограничивающие значения атрибутов безопасности, заданных по умолчанию.

В СЗИ ИС должна быть реализована возможность изменения заданных по умолчанию значений, запроса, модификации, удаления, очистки над конфигурационными параметрами только уполномоченным администраторам.

В СЗИ ИС должна быть реализована возможность осуществлять политику управления доступом к настройкам средств безопасности, чтобы обеспечить ограничивающие значения атрибутов безопасности, заданных по умолчанию.

При создании объекта или информации уполномоченному администратору должно быть позволено определять альтернативные начальные значения атрибутов безопасности вместо заданных по умолчанию.

#### 4.2.4.2. Требования по обеспечению обновления объектов информационной системы

Должен осуществляться контроль следующих элементов СЗИ ИС:

* конфигураций системы с целью мониторинга и анализа параметров настройки ПО и средств защиты;
* контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
* контроль за использованием в СЗИ ИС.

Обновление программного обеспечения ИС должно выполняться в соответствии с утвержденным директором Заказчика регламентом.

#### 4.2.4.3. Требования по обеспечению контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы

Основные активы, ресурсы и оборудование ИС должны быть расположены в зоне контроля физического доступа. Факт наличия контролируемой зоны частично исключает возможность утечки информации по техническим каналам, организуемой нарушителем с базовым потенциалом нападения. Контроль и управление физическим доступом в контролируемую зону должен осуществляться организационно-техническими методами, принятыми в организации владельца ИС.

ИС должны размещаться на серверах, физически размещенных на территории Республики Беларусь.

Задачи безопасности для инженерной инфраструктуры:

1. Должны быть организованы зоны контролируемого доступа:

* одна или несколько зон для размещения оборудования;
* одна или несколько зон для организации рабочих мест персонала ЦОД и Заказчика;
* контролируемая зона для проведения погрузочно-разгрузочных работ.

1. Доступ в контролируемые зоны должен предоставляться только уполномоченному персоналу.
2. Доступ сторонних лиц в контролируемые зоны должен предоставляться только в сопровождении уполномоченного персонала.
3. Должен контролироваться внос и вынос оборудования СЗИ ИС за пределы и между контролируемыми зонами.
4. Должно осуществляться видеонаблюдение за контролируемыми зонами, включая точки входа/выхода каждой зоны.
5. Должна обеспечиваться защита от сбоев и отказов в системах энергообеспечения.
6. Должна обеспечиваться противопожарная защита.
7. Должна обеспечиваться защита инженерной инфраструктуры ЦОД от угроз со стороны окружающей физической среды (гроза, ураган).
8. Должны быть предусмотрены меры защиты, направленные на предотвращение возможных террористических актов.

Требования к обеспечению контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты СЗИ ИС должны соответствовать политике информационной безопасности Заказчика.

#### 4.2.4.4. Требования по обеспечению синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации

Синхронизация временных меток и системного времени для целей аудита событий должна осуществляться посредством NTP-сервера с использованием государственного эталона времени.

### 4.2.5. Требования по обеспечению криптографической защиты информации

#### 4.2.5.1. Требования по обеспечению конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования)

Для организации защищенных каналов связи должны использоваться криптографические средства защиты, обеспечивающие надежную аутентификацию сторон, участвующих в обмене данными, и шифрование их сетевого трафика путем организации VPN канала передачи данных.

Для защиты каналов связи, обеспечивающих взаимодействие с удаленными АРМ администраторов, должны использоваться средства криптографической защиты информации, имеющие сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY).

### 4.2.6. Требования по обеспечению защиты информации в виртуальной инфраструктуре

#### 4.2.6.1. Требования по обеспечению от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг

Распределение вычислительных ресурсов для безотказной работы каждой из виртуальных машин должно обеспечиваться таким образом, чтобы избежать их монополизации и не допустить истощения.

Для СЗИ Платформы ИС должны быть назначены максимальные нормы следующих ресурсов: объем оперативной памяти, объем дискового пространства, количество процессорных ядер для создаваемых виртуальных машин так, чтобы они могли использовать выделяемые ресурсы одновременно.

#### 4.2.6.2. Требования по обеспечению защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин

Политика ролевого управления доступом СЗИ ИС должна осуществляться для субъектов:

* администратор СЗИ;

Все операции между любыми субъектами и любыми объектами должны покрываться политикой управления доступом.

Должна осуществляться политика управления доступом виртуальных машин ресурсов СЗИ ИС к объектам на основании следующего:

* атрибутов безопасности субъекта: атрибуты процесса ВМ;
* атрибутов безопасности объекта: атрибуты ресурса ВМ.

На хостах виртуальной инфраструктуры СЗИ ИС должен быть обеспечен антивирусный контроль с целью защиты от вредоносного кода виртуальных машин на физических серверах среды виртуализации.

Предоставление доступа к функциям управления антивирусным контролем виртуальной инфраструктуры должен быть предоставлен только уполномоченному администратору безопасности.

Обновления базы данных признаков вредоносного программного обеспечения должны осуществляться согласно установленному регламенту.

#### 4.2.6.3. Требования по обеспечению безопасного перемещения виртуальных машин и обрабатываемых на них данных

В СЗИ ИС должно быть гарантировано выполнение всех функций среды виртуализации ресурсов за счет использования механизма миграции виртуальных машин с хоста А на хост В при сбоях, которые сохраняют работоспособное состояние хоста А, например отказ вентилятора процессора, отказ одного из блоков питания и т.д.

В случае, когда автоматическое восстановление после сбоя критичного количества хостов виртуальных машин невозможно, СЗИ ИС должны войти в такой режим функционирования, который обеспечивает возможность ее возврата к безопасному состоянию за счет использования резервных копий виртуальных машин.

#### 4.2.6.4. Требования по обеспечению резервного копирования пользовательских виртуальных машин

В СЗИ ИС должно обеспечиваться резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры с целью сохранения доступности ресурсов виртуальной инфраструктуры в случае сбоев и отказов.

Должно обеспечиваться резервное копирование данных и ПО СЗИ ИС с целью восстановления информации в случае нарушения целостности данных в результате сбоев и отказов физических и виртуальных ресурсов СЗИ ИС.

Для СЗИ ИС в соответствии с установленным регламентом должно осуществляться резервное копирование:

* конфигурации виртуальной инфраструктуры;
* дистрибутивов средств построения виртуальной инфраструктуры;
* ПО серверов управления виртуализацией, АРМ администратора управления средствами виртуализации;
* виртуальных машин, файлов, содержащих параметры настройки виртуальных машин;
* программного обеспечения, настроек средств защиты информации.

#### 4.2.6.5. Требования по обеспечению резервирования сетевого оборудования по схеме N+1

В СЗИ ИС должно обеспечиваться резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры с целью сохранения доступности ресурсов виртуальной инфраструктуры в случае сбоев и отказов. В СЗИ ИС должно обеспечиваться резервирование сетевого оборудования должно осуществляться по принципу N+1.

#### 4.2.6.6. Требования по обеспечению физической изоляции сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам

В СЗИ ИС должно быть обеспечена физическая изоляция информационных систем, относящимся к различным классам информационных систем, на уровне вычислительных ресурсов, ресурсов хранения.

### 4.2.7. Иные требования

#### 4.2.7.1. Требования по определению перечня разрешенного программного обеспечения и регламентация порядка его установки и использования

В составе СЗИ ИС должно использоваться только разрешенное ПО. Состав и контроль ПО должен регламентируются принятыми в организации нормативными документами и программно-техническими средствами.

#### 4.2.7.2. Требования по обеспечению контроля за составом объектов информационной системы

Должен обеспечиваться контроль за составом объектов СЗИ ИС с целью мониторинга и анализа объектов, а также средств защиты СЗИ ИС.

Должен обеспечиваться контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

В составе СЗИ ИС должно использоваться только разрешенное ПО. Должны отсутствовать средства разработки, отладки и модификации программного кода. Состав и контроль ПО должен регламентируются принятыми в организации нормативными документами и программно-техническими средствами.

Уполномоченные администраторы должны иметь в наличии актуальную схему сети с указанием объектов, внешних подключений и информационных потоков ИС.

#### 4.2.7.3. Требования по автоматизированному контролю за составом средств вычислительной техники и сетевого оборудования

Автоматизированный контроль за составом средств вычислительного оборудования ИС должен осуществляться средствами ЦОД.

Оборудование сетевой инфраструктуры является динамически изменяемой средой, предполагаемой внесения изменений в состав оборудования сетевой инфраструктуры без изменения технологии обработки защищаемой информации.

#### 4.2.7.4. Требования по использованию объектов информационной системы под пользовательскими учетными записями

Использование административных учетных записей в СЗИ ИС должно быть строго регламентировано. Такие учетные записи должны использоваться только в случае настройки СЗИ ИС. Требования к порядку использования в СЗИ ИС административных учетных записей должны соответствовать политике информационной безопасности Заказчика.

#### 4.2.7.5. Требования по определению состава и содержания информации, подлежащей резервированию

Резервированию подлежит вся информация, обрабатываемая в информационной системе.

Резервное копирование конфигурационных настроек средств защиты информации, сетевых устройств, системного и прикладного ПО управления виртуализацией должно выполняться выполняется собственными средствами резервного копирования.

#### 4.2.7.6. Требования по обеспечению резервирования информации, подлежащей резервированию

Резервное копирование может производиться следующими способами:

* вручную (оператор, ответственный за резервное копирование запускает процедуру резервного копирования);
* автоматически (запуск производится по расписанию автоматически).

Резервное копирование БД должно производится не реже 1 раза в сутки. Срок хранения резервной копии БД должен составлять не менее 7 дней.

Материально-технические средства системы резервного копирования должны обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью. Лица, ответственные за организацию резервного копирования, должны ежедневно осуществлять контроль за наличием необходимого для резервного копирования объема дискового пространства.

Порядок резервирования информации в СЗИ ИС должен быть строго регламентирован. Требования к резервированию информации СЗИ ИС должны соответствовать политике информационной безопасности Заказчика.

#### 4.2.7.7. Требования по обеспечению резервирования конфигурационных файлов сетевого оборудования

В СЗИ ИС должен обеспечиваться контроль за неизменностью конфигурационных файлов сетевого оборудования.

Резервное копирование конфигурационных файлов сетевого оборудования может выполняться собственными средствами резервного копирования.

К срокам хранения конфигурационных файлов сетевого оборудования предъявляются следующие требования:

* хранение конфигурационных файлов сетевого оборудования СЗИ ИС не менее 1 (одного) года.

#### 4.2.7.8. Требования по обеспечению обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления

Порядок обновления программного обеспечения, а также контроль за своевременностью такого обновления в СЗИ ИС должен быть строго регламентирован. Требования к обновлению программного обеспечения СЗИ ИС должны соответствовать политике информационной безопасности Заказчика".

#### 4.2.7.9. Требования по обеспечению сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных

В СЗИ Платформы ИС для сохранения управляемости системы должно быть организовано разделение всей сети ИС на сеть данных, по которой осуществляется передача всех данных облачных сервисов, и сеть управления, по которой передаются данные управления (администрирования) оборудованием и ПО СЗИ ИС.

На уровне мониторинга и управления настройками оборудования СЗИ ИС должны использоваться выделенные коммутаторы, которые будут обеспечивать передачу трафика управления устройствами по отдельным каналам связи.

#### 4.2.7.10. Требования по обеспечению защиты средств вычислительной техники от вредоносных программ

В целях обеспечения защиты средств вычислительной техники от вредоносных программ в СЗИ ИС должна быть реализована функция антивирусной защиты.

Функции антивирусной защиты должны быть реализованы для следующих элементов СЗИ ИС:

* для защиты серверов и рабочих станций СЗИ ИС;
* для защиты объектов виртуальной среды.

Антивирусное программное обеспечение должно обеспечивать комплексную защиту компьютера от различного вида угроз, сетевых и мошеннических атак.

К компонентам контроля относятся следующие компоненты программы:

а) Контроль запуска программ. Антивирусное программное обеспечение должно отслеживать попытки запуска программ пользователями и регулировать запуск программ;

б) Контроль активности программ. Антивирусное программное обеспечение должно регистрировать действия, совершаемые программами в операционной системе, и регулировать деятельность программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ должен быть задан набор правил. Эти правила должны регламентировать доступ программ к ресурсам операционной системы;

в) Мониторинг уязвимостей. Мониторинг уязвимостей в режиме реального времени должен проверять программы, запущенные на компьютере пользователя, а также проверять программы в момент их запуска;

г) Контроль устройств. Антивирусное программное обеспечение должно установить гибкие ограничения доступа к устройствам, являющимся источниками информации;

д) Веб-Контроль. Антивирусное программное обеспечение должно позволять установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

Работа компонентов контроля должна быть основана на правилах:

* контроль запуска программ должен использовать правила контроля запуска программ;
* контроль активности программ должен использовать правила контроля активности программ;
* контроль устройств должен использовать правила доступа к устройствам и правила доступа к шинам подключения.

Антивирусное программное обеспечение для виртуальных сред должно предусматривать вариант развертывания с легкий агентом, устанавливаемым на каждую виртуальную машину, и позволять использовать расширенный функционал для обеспечения безопасности ВМ, в том числе мониторинг уязвимостей, контроль программ, устройств и веб‑контроль, проверку IM-сообщений, почтовый и веб-антивирус, а также передовые эвристические методы защиты. Вместе эти компоненты антивирусного программного обеспечения не должны снижать производительность виртуальной среды.

#### 4.2.7.11. Требования по обеспечению управления внешними информационными потоками (маршрутизация) между информационными системами

В СЗИ Платформы ИС должен обеспечиваться контроль за информационными потоками на внешних интерфейсах и защита сетевого периметра при ее взаимодействии с внешними информационными системами и при использовании сетей электросвязи общего пользования, в том числе глобальной компьютерной сети Интернет с применением маршрутизатора (коммутатора маршрутизирующего).

#### 4.2.7.12. Требования по обеспечению ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями

Функция межсетевого экранирования должна применяться в целях контроля входящего и исходящего трафика, а также распределения сетевых потоков внутри СЗИ ИС и решать следующие задачи:

* поддержка санкционированных входящих и исходящих соединений;
* ограничение несанкционированной передачи данных в и за пределы системы;
* разделение сетевых потоков в системе;
* управление сетевыми потоками;
* контроль и фильтрация содержимого сетевого обмена;
* защита сетевого периметра от сетевых атак;
* протоколирование событий, связанных с сетевым обменом данными и работой подсистемы.

Фильтрация трафика должна осуществляться на основе настраиваемых стандартных и пользовательских политик безопасности, содержащих наборы правил. Каждое правило в соответствии с категорией безопасности должно содержать настраиваемые зоны безопасности, целевые объекты (все объекты, серверы, сети, сетевые адреса и т.д.), используемые приложения и протоколы, действия (принятие, отказ, сброс). Необходимо, чтобы правила распространялись как на транзитные обрабатываемые потоки, так и на входящие управляющие соединения (ограничение портов, протоколов и сетевых адресов для удаленного администрирования).

#### 4.2.7.13. Требования по обеспечению ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями

В СЗИ ИС должно обеспечиваться межсетевое экранирование с целью:

* ограничения входящего и исходящего трафика только необходимыми соединениями;
* защиты периметра ИС при ее взаимодействии с иными информационными системами и при использовании сетей общего пользования, в том числе Интернет;
* ограничения количества точек доступа в ИС из внешних ИС и сетей до минимально необходимого числа для решения постановленных задач при обеспечении постоянного и всестороннего контроля входящих и исходящих информационных потоков;
* прекращения сетевых соединений по их завершении или по истечении заданного временного интервала неактивности сетевого соединения;
* управления и контроля подключений при взаимодействии с информационными системами третьих лиц;
* контекстная фильтрация данных на уровне протоколов и файлов;
* контекстная фильтрация данных на уровне сигнатур, шаблонов и иных методов.

#### 4.2.7.14. Требования по обеспечению обнаружения и предотвращения вторжений в информационной системе

В СЗИ ИС должно обеспечиваться обнаружение вторжений на сетевом и транспортном уровне с использованием сигнатурного метода анализа, с целью:

* обнаружения в режиме реального времени несанкционированной сетевой активности;
* определения подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
* выявления, анализа и блокирования скрытых каналов передачи информации внутри разрешенных сетевых протоколов;
* фильтрации (обнаружения и очистки) сетевого трафика от вредоносного программного обеспечения.

Должны осуществляться регламентированные обновления базы сигнатур программного средства обнаружения вторжений.

Должна обеспечиваться регистрация событий, возникающих при срабатывании правил обнаружения вторжений и предоставление права просмотра записей аудита только уполномоченному администратору безопасности.

Должна обеспечиваться возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченного администратора безопасности.

#### 4.2.7.15. Требования по определению перечня внешних подключений к информационной системе и порядка такого подключения

Все соединения с удаленными доверенными ИТ-системами физически и логически должны быть защищены средствами СЗИ ИС таким образом, чтобы гарантировать защиту целостности и конфиденциальности передаваемых данных, а также подлинность взаимодействующих сторон. Взаимодействие с внешними информационными системами должно быть строго регламентировано и контролироваться.

Для соединений с удаленными доверенными ИТ-системами должны поддерживаться целостность и конфиденциальности передаваемых данных, а также подлинность взаимодействующих сторон.

Должно обеспечиваться предоставление доступа к настройкам средств межсетевого экранирования, активного сетевого оборудования СЗИ ИС только уполномоченному администратору безопасности из доверенного сетевого сегмента СЗИ ИС.

#### 4.2.7.16. Требования по обеспечению контроля за внешними подключениями к информационной системе

В СЗИ ИС должно обеспечиваться межсетевое экранирование с целью:

* ограничения входящего и исходящего трафика только необходимыми соединениями, согласно политике межсетевого взаимодействия;
* защиты периметра СЗИ ИС при ее взаимодействии с иными информационными системами и при использовании сетей общего пользования, в том числе Интернет;
* деления информационной системы на сегменты и обеспечения защиты периметров сегментов информационной системы;
* ограничения количества точек доступа в СЗИ ИС из внешних ИС и сетей до минимально необходимого числа для решения постановленных задач при обеспечении постоянного и всестороннего контроля входящих и исходящих информационных потоков;
* прекращения сетевых соединений по их завершении или по истечении заданного временного интервала неактивности сетевого соединения;
* управления и контроля подключений при взаимодействии с информационными системами третьих лиц;
* контекстная фильтрация данных на уровне протоколов и файлов;
* контекстная фильтрация данных на уровне сигнатур, шаблонов и иных методов.

#### 4.2.7.17. Требования к проведению внешней и внутренней проверки информационной системы

Проведение проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности СЗИ ИС и сведения о которых подтверждены изготовителями (разработчиками) этих объектов должно осуществляться с применением лицензионного средства сканирования, имеющего сертификат соответствия требованиям технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/ВY).

Данные проверки должны проводиться в соответствии с утвержденным Заказчиком графиком, но не реже 1 (одного) раза в год.

# 

# 5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СЗИ ИС

Стадии и этапы работ по созданию СЗИ ИС, а также содержание и результаты этих работ представлены в таблице 5.1.

Таблица 5.1. – Стадии и этапы работ

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Наименование этапа** | **Состав и результаты работ** |
| 1. | Проектирование системы защиты информации информационной системы | 1. Проект акта по отнесению информационной системы к классу типовых информационных систем в порядке, установленном СТБ 34.101.30-2017.  2. Техническое задание на систему защиты информации. |
| 2. | Создание системы защиты информации информационной системы | 1. Политика информационной безопасности (политика верхнего уровня).  2. Политика использования электронной почты.  3. Политика контроля/мониторинга над функционированием ИС.  4. Политика обновления средств защиты информации.  5. Политика по организации антивирусной защиты  6. Политика реагирования на инциденты информационной безопасности.  7. Политика резервирования и хранения данных. |
| 3. | Аттестация системы защиты информации информационной системы | 1. Исходные данные в соответствии с требованиями приказа ОАЦ от 20.02.2020 № 66.  2. Программа аттестации СЗИ Информационной системы.  3. Программа и методика проведения испытаний.  4. Протокол испытаний.  5. Технический отчет.  6. Аттестат соответствия СЗИ Информационной системы требованиям по защите информации. |

# 6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

До ввода СЗИ Платформы ИС в эксплуатацию должны быть проведены следующие виды испытаний:

* опытная эксплуатация;
* приемочные испытания;
* аттестация СЗИ.

## 6.1. Виды испытаний системы

Опытная эксплуатация СЗИ ИС производится с целью определения готовности персонала Заказчика к постоянной эксплуатации СЗИ ИС, уточнения количественных и качественных характеристик СЗИ ИС, корректировки (при необходимости) документации.

Приемочные испытания СЗИ ИС проводятся с целью определения соответствия СЗИ ИС ТЗ и принятия решения о возможности перевода СЗИ ИС в постоянную эксплуатацию. Приемочным испытаниям СЗИ ИС должна предшествовать опытная эксплуатация.

### 6.1.1. Состав, объем и методы испытаний системы

Состав, объем и методы приемочных испытаний СЗИ ИС определяются Программой и методикой испытаний, разрабатываемой на стадии ввода в действие. Приемочные испытания ИС должны подвергать проверке компоненты, устанавливаемые в ходе работ по вводу в действие СЗИ ИС. При проведении приемочных испытаний проверяется качество выполнения компонентами СЗИ ИС своих функций в различных режимах функционирования в соответствии с Программой и методикой испытаний. Проведение всех видов испытаний СЗИ ИС не должно вызвать сбоев в работе Заказчика.

### 6.1.2. Опытная эксплуатация системы

Опытная эксплуатация СЗИ ИС производится на этапе подготовки к испытаниям. Программа опытной эксплуатации определяет:

* условия и порядок функционирования компонентов СЗИ ИС;
* продолжительность опытной эксплуатации;
* порядок устранения недостатков, выявленных в процессе опытной эксплуатации.

### 6.1.3. Приемочные испытания системы

Приемочные испытания СЗИ ИС проводятся после завершения опытной эксплуатации СЗИ Платформы ИС.

Приемочные испытания должны проводиться на функционирующих компонентах СЗИ ИС.

### 6.1.4. Аттестация системы защиты информации

Аттестация СЗИ ИС проводится после завершения приемочных испытаний СЗИ ИС.

Порядок аттестации СЗИ ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам определяется положением о порядке аттестации СЗИ ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

Аттестация СЗИ предусматривает комплексную оценку СЗИ в реальных условиях эксплуатации ИС и включает:

* разработку программы и методики аттестации;
* установление соответствия реального состава и структуры объектов информационной системы общей схеме СЗИ;
* проверку правильности отнесения ИС к классу типовых ИС, выбора и применения СЗИ;
* анализ разработанной документации на СЗИ собственника (владельца) информационной системы на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации;
* ознакомление с документацией о распределении функций персонала по организации и обеспечению защиты информации;
* проведение испытаний СЗИ на предмет выполнения установленных законодательством требований по защите информации;
* внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС;
* оформление технического отчета и протокола испытаний;
* оформление аттестата соответствия.

Программа и методика аттестации разрабатываются на основании исходных данных и должны содержать перечень выполняемых работ, методов проверки требований безопасности, реализованных в СЗИ, используемой контрольной аппаратуры и тестовых средств, а также информацию о продолжительности их выполнения.

Технический отчет должен содержать:

* сроки проведения испытаний;
* вывод о соответствии (несоответствии) реального состава и структуры объектов ИС общей схеме СЗИ;
* вывод о выполнении (невыполнении) установленных законодательством требований по защите информации;
* отчет о внешней и внутренней проверке отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов ИС.

При подтверждении соответствия СЗИ требованиям законодательства об информации, информатизации и защите информации оформляется аттестат соответствия сроком на пять лет.

## 6.2. Общие требования к приемке работ по стадиям

Общие требования к виду, составу, объему работ и методам испытаний СЗИ ИС устанавливается программой и методикой испытаний, а также программой опытной эксплуатации, разрабатываемой на этапе подготовки к испытаниям СЗИ ИС.

### 6.2.1. Перечень участвующих предприятий и организаций

Участниками приемочных испытаний являются:

* Заказчик;
* Исполнитель.

### 6.2.2. Место и сроки проведения испытаний

Все испытания, а также мероприятия по аттестации СЗИ ИС проводятся на территории Заказчика.

### 6.2.3. Порядок согласования и утверждения приемочной документации

Приемочные испытания СЗИ Платформы ИС проводятся комиссией, состав которой утверждается управляющим Заказчика.

Председателем комиссии назначается представитель Заказчика.

Протоколы проведения испытаний подписываются всеми членами комиссии.

При положительном результате проведения приемочных испытаний составляется акт о введении системы в промышленную эксплуатацию. Акты подписываются всеми членами комиссии.

# 7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ

Для создания условий функционирования СЗИ ИС, при которых гарантируется соответствие создаваемой СЗИ требованиям, содержащимся в настоящем документе, и возможности эффективного использования СЗИ, на объектах автоматизации должны быть предусмотрены следующие мероприятия:

1. Обеспечение силами Заказчика выделения вычислительных мощностей, требования к которым определены в разделе 4.1 настоящего ТЗ, а также установки необходимого ПО. Требования по характеристикам оборудования должны быть уточнены на этапе технического проектирования.
2. Обеспечения силами Заказчика необходимой сетевой инфраструктуры, включая защищенные каналы связи.
3. Получение силами заказчика криптографических ключей и сертификатов для шифрования.
4. Обеспечение процесса подготовки персонала Заказчика по следующей схеме:

* Исполнитель обеспечивает подготовку политик;
* Заказчик согласовывает политики информационной безопасности;
* Заказчик обеспечивает внедрение политик информационной безопасности;
* Заказчик обеспечивает обучение конечных пользователей.

# Приложение 1

**к Техническому заданию на создание системы защиты ИС**

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Наименование требования** | **Пункт требования приказа ОАЦ № 66** |
|
| **1.** | **Аудит безопасности** | |
| 1.1. | Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое) | 4.2.1.1. |
| 1.2. | Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года | 4.2.1.2. |
| 1.3. | Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года | 4.2.1.3. |
| 1.4. | Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы | 4.2.1.4. |
| 1.5 | Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года | 4.2.1.5 |
| **2.** | **Требования по обеспечению защиты данных** | |
| 2.1. | Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием | 4.2.2.1. |
| 2.2. | Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации | 4.2.2.2. |
| 2.3. | Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности | 4.2.2.3. |
| **3.** | **Требования по обеспечению идентификации и аутентификации** | |
| 3.1. | Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации | 4.2.3.1. |
| 3.2. | Обеспечение идентификации и аутентификации пользователей информационной системы | 4.2.3.2. |
| 3.3. | Обеспечение защиты обратной связи при вводе аутентификационной информации | 4.2.3.3. |
| 3.4. | Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы | 4.2.3.4. |
| 3.5. | Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы | 4.2.3.5. |
| 3.6. | Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы | 4.2.3.6. |
| 3.7. | Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу | 4.2.3.7. |
| **4.** | **Требования по защите системы защиты информации информационной системы** | |
| 4.1. | Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию | 4.2.4.1. |
| 4.2. | Обеспечение обновления объектов информационной системы | 4.2.4.2. |
| 4.3. | Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы | 4.2.4.3. |
| 4.4. | Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации | 4.2.4.4. |
| **5.** | **Обеспечение криптографической защиты информации** | |
| 5.1. | Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования) | 4.2.5.1. |
| 5.2. | Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования) | - |
| 5.3. | Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи) | 4.2.5.3. |
| 5.4. | Обеспечение контроля целостности данных в информационной системе (средства контроля целостности) | - |
| 5.5. | Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены) | - |
| 5.6. | Обеспечение идентификации и аутентификации в информационной системе (криптографические токены) | - |
| **6.** | **Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре** | |
| 6.1. | Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг | 4.2.6.1. |
| 6.2. | Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин | 4.2.6.2. |
| 6.3. | Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных | 4.2.6.3. |
| 6.4. | Обеспечение резервного копирования пользовательских виртуальных машин | 4.2.6.4. |
| 6.5. | Обеспечение резервирования сетевого оборудования по схеме N+1 | 4.2.6.5. |
| 6.6. | Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам | 4.2.6.6. |
| **7.** | **Иные требования** | |
| 7.1. | Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования | 4.2.7.1. |
| 7.2. | Обеспечение контроля за составом объектов информационной системы | 4.2.7.2. |
| 7.3. | Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования | 4.2.7.3. |
| 7.4. | Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы) | 4.2.7.4. |
| 7.5. | Определение состава и содержания информации, подлежащей резервированию | 4.2.7.5. |
| 7.6. | Обеспечение резервирования информации, подлежащей резервированию | 4.2.7.6. |
| 7.7. | Обеспечение резервирования конфигурационных файлов сетевого оборудования | 4.2.7.7. |
| 7.8. | Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления | 4.2.7.8. |
| 7.9. | Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных | 4.2.7.9. |
| 7.10. | Обеспечение защиты средств вычислительной техники от вредоносных программ | 4.2.7.10. |
| 7.11. | Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ | 4.2.7.11. |
| 7.12. | Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ | 4.2.7.12. |
| 7.13. | Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего) | 4.2.7.13. |
| 7.14. | Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях | 4.2.7.14. |
| 7.15. | Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях | 4.2.7.15. |
| 7.16. | Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений | 4.2.7.16. |
| 7.17. | Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений | - |
| 7.18. | Обеспечение обнаружения и предотвращения утечек информации из информационной системы. Использование системы обнаружения и предотвращения утечек информации из информационной системы | - |
| 7.19. | Определение перечня внешних подключений к информационной системе и порядка такого подключения | 4.2.7.18. |
| 7.20. | Обеспечение контроля за внешними подключениями к информационной системе | 4.2.7.19. |
| 7.21. | Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы | 4.2.7.20. |

**Лист регистрации изменений**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Изм. | Номера листов (страниц) | | | | Всего листов (стр.) в документе | № документа | Входящий  № сопроводите-льного документа | Подпись | Дата |
| изме­ненных | Замененных | новых | Аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**СОСТАВИЛИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование организации, предприятия** | **Должность** | **Фамилия, имя, отчество** | **Подпись** | **Дата** |
| ООО "Активные технологии" | Ведущий специалист по защите информации | А.В. Грецкий. |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**СОГЛАСОВАНО**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование организации, предприятия** | **Должность** | **Фамилия, имя, отчество** | **Подпись** | **Дата** |
| Заказчик |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |