1. **Общие сведения**

Настоящее Техническое задание разработано в соответствии с приказом №62 «О некоторых вопросах технической и криптографической защиты информации» оперативно-аналитического центра при президенте республики беларусь и является основным документом, определяющим требования и порядок создания, развития, модернизации, сопровождения Системы защиты информации информационной системы класс Б2.

Результатом создания системы защиты информации информационной системы класс Б2 должна стать полностью работоспособная автоматизированная система защиты информации информационной системы класса Б2, соответствующая требованиям настоящего технического задания.

**1.1 Полное наименование системы**

Полное наименование системы – «Системы защиты информации информационной системы класс Б2».

**1.2 Наименование реквизитов разработчика и заказчика СЗИ ИСПДн.**

Заказчик: Белорусский государственный университет. Адрес: 220000, проспект Независимости 4, Минск.

Испольнитель: ООО «Рокет Эпс» Адрес: 220000, Бизнес-центр Альянс, 3-я улица Щорса 9, Минск

**1.3 Перечень документов, на основании которых создаётся СЗИ ИСПДн.**

Для формирования требований были использованы документы, разработанные на предыдущих этапах создания СЗИ, которые приведены в таблице 1.

Таблица 1. Документы, разработанные на предыдущих этапах создания СЗИ

|  |  |
| --- | --- |
| № п/п | Наименование документа |
| 1 | Классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами; |
| 2 | Акт классификации системы защиты информации |

Основные руководящие и нормативно – технические документы приведены в таблице 2.

Таблица 2. Перечень основных руководящих и нормативно технических документов.

|  |  |
| --- | --- |
| № п/п | Наименование документа |
|  | СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель». |
|  | СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности». |
|  | СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности». |
|  | СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования». |
|  | СТБ 34.101.9-2004 «Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы». |
|  | СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». |

Плановые сроки начала и окончания работ по созданию системы защиты информации:

Начало работ – 01 декабря 2016 года. Окончание работ – 01 апреля 2017 года.

**2. Назначение и цели создания системы**

**2.1 Назначение системы защиты.**

СЗИпредназначена для сотрудников Белорусского государственного университета.

**2.1 Цели создания системы защиты**

Целями создания системы защиты ИСПД является защита информации кафедры телекоммуникаций и информационных технологий факультета Радиофизики и компьютерных технологий БГУ.

Критерием оценки достижения целей создания системы является снижение величины наносимого ущерба вследствие реализации угроз безопасности, путём применения технических, организационных мер, надлежащее выполнение требований безопасности, предусмотренных нормативно-методическими документами.

**2.2 Краткая характеристика информационной системы, структура**.

Информационная система представляет из себя кафедру высшего учебного заведения.

**2.3 Размещение СЗИ*.***

СЗИ будет расположена по адресу ул. Курчатова 5, Минск.

**2.4 Охрана и пропускной режим.**

На объекте, на котором планируется внедрить систему защиты информации осуществляется контрольно-пропускной режим. Так же вход и выход с объекта ограничен с 23:00 до 7:00.

**2.5 Контролируемая зона.**

Контролируемая зона представлена в виде периметра стен помещений, располагающихся на 5 этаже учебного корпуса РФиКТ.

**2.6 Схема информационного взаимодействия объектов в ИС.**

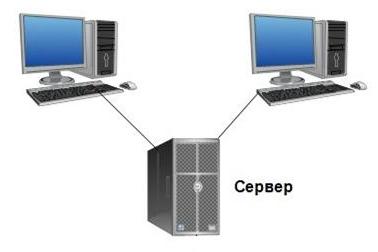


Рисунок 1. Схема информационного взаимодействия объектов

Информационная система не имеет выхода в сети общего пользования.

**2.7. Частная модель угроз безопасности в ИС**

* разглашение экзаменационных билетов
* изменение экзаменационных билетов
* хищение персональных данных студентов
* уничтожение персональных данных студентов
* модификация персональных данных студентов
* модификация сведений об успеваемости
* хищение личных данных сотрудников
* уничтожение личных данных сотрудников
* модификация личных данных сотрудников
* изменение нагрузки преподавателей
* изменение часовой оплаты занятий
* копирование научно-исследовательская работ

**3 Требования к системе защиты информации ИС**

**3.1 Требования к функциям (задачам), выполняемым системой.**

* Идентификация объектов информационной системы (далее – объекты) и закрепление за ними субъектов информационной системы (далее – субъекты)
* Идентификация и аутентификация субъектов
* Управление идентификаторами, в том числе создание, присвоение, уничтожение
* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
* Исключение отображения аутентификационной информации
* Изменение атрибутов безопасности, установленных по умолчанию в соответствии с политикой информационной безопасности
* Полномочное управление (создание, активация, блокировка и уничтожение) учетными записями субъектов
* Определение прав и обязанностей субъектов
* Реализация правил разграничения доступа субъектов к объектам
* Блокирование доступа к информационной системе после истечения установленного времени бездействия (неактивности) субъекта или по его запросу
* Определение при необходимости действий субъектов, которые могут совершаться такими субъектами до их идентификации и аутентификации
* Наличие актуальной схемы сети с указанием объектов, внешних подключений и информационных потоков
* Управление (фильтрация, маршрутизация, контроль соединений) информационными потоками между объектами, а также между информационными системами
* Ограничение входящего и исходящего трафика только необходимыми соединениями
* Запрет на использование в информационной системе технологий беспроводного доступа
* Регламентация порядка использования в информационной системе мобильных технических средств и контроля за таким использованием
* Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования
* Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования
* Регламентация доступа к учтенным машинным носителям информации
* Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на учтенных машинных носителях информации
* Уничтожение (удаление) данных с машинных носителей информации при их передаче лицам, не являющимся субъектами информационной системы, в том числе для ремонта, технического обслуживания
* Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
* Сбор, запись и хранение информации о событиях безопасности в течение установленного срока хранения
* Мониторинг (просмотр, анализ) событий безопасности уполномоченными субъектами
* Сбор, запись и хранение, а также мониторинг (просмотр, анализ) информации о сбоях в механизмах сбора информации и достижении предела объема (емкости) памяти устройств хранения уполномоченными пользователями
* Синхронизация временных меток и (или) системного времени в информационной системе
* Защита информации о событиях безопасности
* Защита информации о событиях безопасности
* Регламентация обновления базы данных признаков вредоносного программного обеспечения
* Регламентация проведения проверок операционных систем на предмет обнаружения аномалий, вызванных присутствием в системе вредоносного программного обеспечения
* Выявление уязвимостей информационной системы и оперативное их устранение
* Контроль за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
* Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации
* Контроль за работоспособностью, параметрами настройки и правильностью функционирования программного обеспечения и средств защиты информации
* Регламентирование порядка резервирования информации и программного обеспечения, включая программное обеспечение средств защиты информации
* Идентификация и аутентификация субъектов и объектов в виртуальной инфраструктуре, в том числе уполномоченных пользователей по управлению средствами виртуализации
* Управление доступом субъектов к объектам в виртуальной инфраструктуре, в том числе внутри виртуальных машин
* Установление контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации
* Контроль и управление физическим доступом внутри контролируемой зоны к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они размещены (установлены), исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, а также в помещения и сооружения, в которых они установлены

**4. Требования к средствам защиты.**

При осуществлении технической защиты информации используются средства технической защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь

**4.1 Требования по электрической и пожарной безопасности**

Технические средства, применяемые для реализации приведённых выше требований должны соответствовать нормам по электрической и пожарной безопасности, принятым на предприятии заказчика.

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование.

**4.2 Требования по эксплуатации и техническому обслуживанию**

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание ПЭВМ. При эксплуатации система должна быть обеспечена соответствующая стандартам хранения носителей и эксплуатации ПЭВМ температура и влажность воздуха. Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств. Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности. Все пользователи системы должны соблюдать правила эксплуатации электронной вычислительной техники. Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Квалификация персонала и его подготовка должны соответствовать технической документации.

**4.3 Требования к патентной чистоте**

По всем техническим и программным средствам, применяемым в системе, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота на территории Республики Беларусь.

Патентная чистота – это юридическое свойство объекта, заключающиеся в том, что он может быть свободно использован в Республике Беларусь без опасности нарушения действующих на ее территории патентов исключительного права, принадлежащего третьим лицам (права промышленной собственности).

**4.4 Требования к эргономике и технической эстетике**

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы. Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен используется главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

**4.5 Требования к составу и содержанию работ по созданию системы защиты информации персональных данных**.

Этапы работы по созданию СЗИ отражены в таблице 4.

Таблица 4.

| Этап | Содержание работ\* | Результаты работ |
| --- | --- | --- |
| 1 | Классификация информации, хранящейся и обрабатываемой в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, в том числе техническими нормативными правовыми актами; |  |
| 2 | Анализ организационной структуры информационной системы и информационных потоков в целях определения состава (количества) и мест размещения элементов системы (аппаратных и программных), ее физических и логических границ; |  |
| 3 | Присвоение информационной системе класса типового объекта информатизации в порядке, установленном СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация»; |  |
| 4 | Определение требований к системе защиты информации в техническом задании на информационную систему | Техническое задание |
| 5 | Согласование технического проекта.  Разработанный технический проект отправляется на ознакомление и согласование заказчику. В ходе этого этапа могут быть внесены дополнения и изменения в проект, если это потребуется. Итогом согласования проекта является подписание его сторонами. |  |
| 6 | Закупка средств защиты информации, указанных в техническом проекте.  На этом этапе производится закупка средств защиты информации, предусмотренных техническим проектом; Средства защиты должны быть закуплены в полном объёме. | Доставка на объект заказчика закупленных средств защиты информации. |
| 7 | Установка и настройка параметров закупленных средств защиты информации.  Закупленные средства защиты должны быть установлены на объекте заказчика и соответствующим образом настроены для выполнения своих функций. Настройка должна производиться специалистами, имеющими соответствующую квалификацию. | Распаковка, монтаж, подключение и настройка параметров средств защиты на объекте заказчика. |
| 8 | Проведение испытаний созданной системы защиты информации | Акт ввода в опытную эксплуатацию. |
| 9 | Составление документации на автоматизированную систему защиты информации, необходимой нормативно-распорядительной документации на объекте информатизации | Технический паспорт на созданную систему защиты информации. Инструкция администратора систем, инструкция пользователя системы. |
| 10 | Аттестация СЗИ | Программа и методика аттестационных испытаний  Протокол аттестационных испытаний  Заключение по результатам аттестационных испытаний  Аттестат соответствия |
| 7 | Ввод системы в эксплуатацию | Акт ввода системы в промышленную эксплуатацию. |

**4.6 Требования к разработчику системы защиты**

Привлекаемый на договорной основе разработчик (юридическое лицо или индивидуальный предприниматель) должен иметь лицензию(ии) на деятельность по технической и (или) криптографической защите информации выдаваемую оперативно-аналитическим центром при Президенте Республики Беларусь.

**5. Порядок контроля и приёмки системы**

**5.1 Порядок проведения приёмки**

Испытания СЗИ проводятся на объекте заказчика;

Испытания могут проводиться с целью проверки как отдельной подсистемы или функционального модуля, так и на СЗИ в целом.

На основании решения о приемке осуществляется подписание комиссией акта приемки;

Опытная эксплуатация системы защиты ИСПД выполняется на развернутом и настроенном рабочем месте, на котором потом будет осуществляться дальнейшая промышленная эксплуатация.