МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 100503 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНАЯ РАБОТА

на тему

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ФОРМИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ EMBOX

Студент Мельников Антон Витальевич

Руководитель Жарков А.Д

Нормоконтролёр Иванов А.П.

Рецензент зам. начальника отделения АО «ПНИЭИ» Сомкин С.А.

Работа допущена к защите (протокол заседания кафедры от 20.06.16 № 14)

Заведующий кафедрой С.Л. Зефиров

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 23.06.16 № 5)

Секретарь ГЭК А.П. Иванов

Пенза 2016

РЕФЕРАТ

Отчет 89с., 2 рис., 15 табл., 8 ист., 1 прил.

ОПЕРАЦИОННАЯ СИСТЕМА, ТЕСТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БИЗНЕСС-ПРОЦЕСС, ИНФОРМАЦИОННЫЙ АКТИВ, УГРОЗА, УЯЗВИМОСТЬ, СЦЕНАРИЙ ИНЦИДЕНТА, ОБРАБОТКА РИСКОВ, ЗАЩИТНАЯ МЕРА

Объектом исследования является применение операционной системы embox в подразделении организации занимающегося тестированием программного обеспечения.

Цель работы – оценка рисков, возникающих при использовании операционной системы embox, и разработка политик ИБ для организации, использующей операционную систему embox.

В процессе работы выполнено описание основных особенностей ОС embox, идентифицирована среда использования, выполнена идентификация угроз и уязвимостей для информационной системы, в которой используется аппаратура с предустановленной embox, на основе корпоративной политики организации разработаны частные политики ИБ для подразделения, использующего аппаратуру с предустановленной embox.

В результате исследований была произведена оценка и анализ риска, разработан перечень организационных мер, осуществлен выбор наиболее актуальных технических средств, выполнена разработка частных политик информационной безопасности.

СОДЕРЖАНИЕ

Введение 5
1 Ознакомление с операционной системой Embox 6
2 Сравнительный анализ Embox с аналогичными операционными системами 15
3 Оценка рисков 19
3.1 Идентификация среды использования операционной системы embox.. 19
3.2 Идентификация активов, угроз ИБ, уязвимостей активов, сценариев инцидентов ИБ 19
3.2.1 Идентификация информационных активов 19
3.2.2 Идентификация угроз информационной безопасности 23
3.2.3 Идентификация уязвимостей активов информационной системы... 25
3.2.4 Идентификация существующих защитных мер 28
3.2.5 Идентификация последствий 29
4 Анализ и оценивание риска информационной безопасности 37
4.1 Анализ риска 37
4.2 Оценивание риска 39
4.3 Выбор защитных мер в заданных областях обеспечения информационной безопасности 41
4.3.1 Определение способов обработки рисков информационной безопасности 41
4.3.2 Выбор защитных мер 44
5 Разработка политик информационной безопасности автоматизированной системы для областей обеспечения информационной безопасности 58
Заключение 59
Список использованных источников 60
ПРИЛОЖЕНИЕ А 61

СПИСОК СОКРАЩЕНИЙ

– ОС – операционная система;

– СПб ГУ – Санкт-Петербургский государственный университет;

– ОС РВ – операционная система реального времени;

– ЭВМ – электронно-вычислительная машина;

– ПО – программное обеспечение;

– ПАК – программно-аппаратный комплекс;

– ИБ – информационная безопасность;

– ИА – информационный актив;

– ВА – вспомогательный актив;

– АО – аппаратное обеспечение;

– БД – база данных;

– УЯ – уязвимость;

– ИН – инцидент;

– СИ – сценарий инцидента;

– ИС – информационная система;

– ТС – техническое средство;

– ОМ – организационная мера;

– ЗМ – защитная мера;

– СЗИ от НСД – средство защиты информации от несанкционированного доступа.

ВВЕДЕНИЕ

В настоящее время вся аппаратура обработки, передачи информации строится с использованием микроконтроллеров, микропроцессоров. Для обеспечения контроля функционирования данных устройств используются операционные системы реального времени. Данные системы позволяют обеспечивать контроль устройств в режиме реального времени, что позволяет избежать ошибок, и нарушения функционирования. На мировом рынке программного обеспечения существует широкий выбор ОС РВ, но в коммерческом плане не всегда выгодно их использование.

Объектом исследования является ОС РВ embox являющаяся разработкой отечественных программистов из СПб ГУ. Данная ОС находится в свободном доступе и обладает лицензией BSD. В настоящее время ведется тестирование данной ОС, производится разработка приложений, и аппаратных средств с предустановленной на них ОС embox.

В процессе проведения исследований осуществлено описание функциональных возможностей ОС, произведена идентификация среды использования данной системы. В дальнейшем были идентифицированы угрозы и уязвимости ИС, в которой применяется аппаратура с ОС embox.

Произведен анализ и оценивание риска, определены способы обработки рисков, и в соответствии с ГОСТ Р ИСО/МЭК 27002-2012 выбраны защитные меры. Также для минимизации вероятности реализации угрозы разработаны организационные меры и выбраны технические средства, которые способствуют минимизации риска.

В результате проделанной работы осуществлены оценка и анализ риска, разработан перечень организационных мер, осуществлен выбор наиболее актуальных технических средств, выполнена разработка частных политик информационной безопасности в областях, интересующих руководство данного подразделения.

1 Ознакомление с операционной системой Embox

Embox - конфигурируемая кросс-платформенная операционная система жесткого реального времени, поддерживающая архитектуры (x86, ARM, MIPS, Microblaze, SPARC, PPC), несколько файловых систем (FAT, ext2/3/4, jffs2, nfs), языки программирования (java, python, lua, lisp, C/C++) [1].

В состав ОС Embox входят: ядро операционной системы, сетевая и файловая службы графическая подсистема библиотеки языка С и совместимости со стандартом POSIX. Весь код ядра ОС Embox располагается в различных компонентах (библиотеках), которые реализуют те или иные интерфейсы, например, интерфейс диспетчера памяти. Только требуемые компоненты системы включаются в конечный образ. Таким образом, достигается создание образа ОС, нацеленного на конкретную задачу, будь то система с ограниченными ресурсами, либо полноценная операционная система, включающая сетевую и файловую подсистемы, а также управление виртуальной памятью. Это достигается за счет высокой конфигурируемости системы, при этом обладающей возможностью проверки корректности заданной конфигурации и системы в целом, что является необходимым условием при разработке надежных систем реального времени. Также модульность ОС влияет на устойчивость системы – вследствие выхода из строя, какого-либо модуля нет необходимости перезагружать всю система

Ключевыми особенностями и возможностями ОС Embox является:

– ОС состоит из модулей, описание которых содержит информацию о требованиях к применению данных модулей, а также их характеристиках и возможностях. Система сборки образа конечной ОС позволяет задавать необходимые характеристики конечной системы, а также автоматически проверять ограничения и разрешать межмодульные зависимости. Это позволяет проводить формальную верификацию как образа в целом, так и каждого компонента в отдельности с использованием статического анализа кода и на основе его формального описания;

– возможность настройки под конкретную задачу позволяет включать в образ только требуемые модули , следовательно позволяет выполняться на большом спектре вычислительных систем (встроенные системы, однокристальные ЭВМ, многопроцессорные и много-машинные комплексы);

– помимо накладывания различных ограничений и зависимостей, определенные модули могут группироваться по предоставляемой ими функциональности, реализуя совместимый интерфейс. Применение понятия интерфейсов обеспечивает возможность создания образа ОС, отвечающего заданным требованиям по функциональности;

– ОС РВ может быть сконфигурирована с учетом архитектуры MILS и в соответствии со стандартом ARINC-653, ОС РВ обеспечивает надежную работу системы в целом на основе работы ненадежных приложений, выполняющихся в изолированном пространстве различных разделов;

– применение независимых модулей позволяет строить двухуровневые системы изоляции и распределения ресурсов (по процессорному времени, по адресному пространству, по прерываниям), что позволяет одновременно производить планирования как по разделам так, и по процессам;

– возможность расширять и добавлять программные интерфейсы обеспечивает поддержку требуемых стандартов для ОС (POSIX стандарты IEEE Std 1003.1, IEEEStd 1003.1b, IEEE Std 1003.1c, а также программному интерфейсу ARINC-653).

Операционная система Embox предназначена для создания конечных систем с повышенными требованиями к надежности выполнения задач, времени безотказной работы и времени реакции на событие.

ОС Embox представляет собой конфигурируемую кроссплатформенную ОС. Код ОС располагается в различных модулях и пакетах. Модули могут быть составными, а также допускают задание различных параметров. Можно представить вертикальное разделение по модулям. Вертикальное разделение представлено на рисунке 1. В этом случае составные модули можно называть слоями или уровнями.

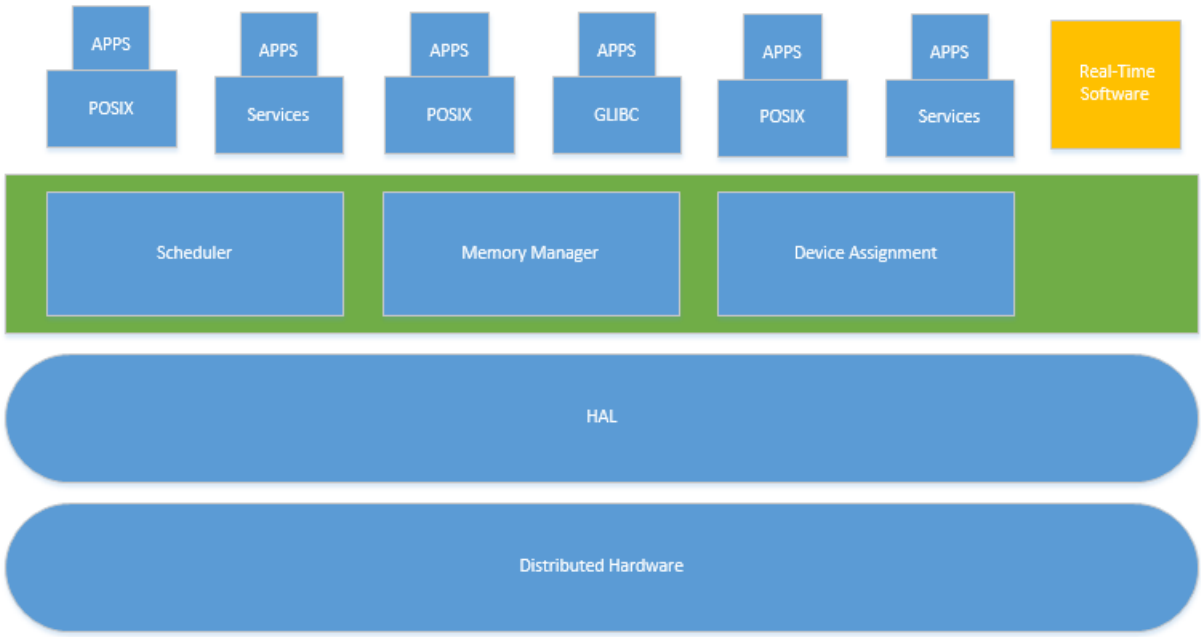

Рисунок 1 – Вертикальное разделение модулей ОС

Каждый элемент данной схемы выполняет заданные функции:

– HAL (Слой аппаратной совместимости) обеспечивает платформозависимые операции и службы, такие как примитивы виртуальной памяти, атомарные операции, источник системных тактов, и так далее.

– ядро обеспечивает управление вычислительными ресурсами системы. Основными ресурсами системы являются процессорное время, память и периферийные устройства. Управление ресурсами может осуществляться на основе различных стратегий. Таким образом, можно выделить ядро разделения (гипервизор), осуществляющее планирование и изоляцию ресурсов на основе статической информации, и ядро раздела. Это может быть ядро ОС общего назначения, например Linux, а также другие платформы с обычными алгоритмами планирования, обеспечивающее работу задач реального времени (с планировщиком реального времени).

– слой аппаратной совместимости состоит из модулей, поддерживающих:

– загрузочный код. Во время старта первым выполняется полностью архитектурнозависимый загрузочный код, чтобы обеспечить первоначальную инициализацию ЦПУ;

– режимы процессора. Абстрагирует режимы процессора, предоставляя интерфейс для доступа к слову состояния процессора, разрешению на прерывания, управление кэшем, и так далее;

– таблица прерывания. Предоставляется интерфейс для управления системной таблицей прерываний, функций получения и установки обработчиков, первичные обработчики прерываний;

– атомарные операции. Предоставляет механизм, с помощью которого можно создавать в программах секции, защищенные от прерывания;

– контекст выполнения (процессора). Позволяет сохранить и восстановить, переключить контекст (состояние нити, достаточное для того, чтобы вернуться к приостановленной нити; используется в псевдомногозадачности);

– виртуальная память. Предоставляет примитивы для работы с аппаратным контроллером памяти (MMU);

– системные устройства:

– контроллер прерываний - интерфейс к аппаратному контроллеру прерываний;

– часы - интерфейс к аппаратному устройству часов.

Реализация этого интерфейса (слоя) достаточна для переноса кода ОС на различные процессорные архитектуры. Для полного переноса на различные аппаратные платформы необходимо реализовать соответствующий набор драйверов [1].

Поскольку слой HAL представляет из себя составной модуль, входящие в него части могут реализоваться независимо. Это позволяет не только ускорить перенос кода на новую платформу, но и реализовывать только требуемые для платформы части, например, не реализовывать поддержку MMU, если в ней нет необходимости или она отсутствует на целевой архитектуре. Такой поход позволяет адаптировать код ОС для работы на широком спектре устройств, от небольших ARM контроллеров, до многоядерных процессоров с поддержкой механизмов виртуализации.

Ядро операционной системы отвечает за планирование, изоляцию и контроль вычислительных ресурсов системы, а также за коммуникацию между различными программными модулями.

Основными ресурсами системы являются:

- процессорное время;
- память;
- аппаратные устройства.

За распределение процессорного времени отвечает планировщик. Он может использоваться в системах с различным количеством и типом процессорных ресурсов:

- одноядерные процессорные системы;
- многоядерные симметричные процессорные системы;
- многоядерные асимметричные процессорные системы;
- симметричные и асимметричные многопроцессорные системы.

В зависимости от распределения задач по процессорам, алгоритмы планировщика выделяют следующие типы стратегий:

- SMP симметричная многопроцессорность. Планировщик выделяет квант времени для задачи на любом из процессоров. Прерывания также выполняются на любом из процессорных ядер;
- AMP асимметричная многопроцессорность. Планировщик выполняет задачи на определенном процессорном ядре, например, обработку прерываний или какие-либо системные задачи;
- BMP ограниченная (задаваемая) многопроцессорность.

Планировщик может выполнять задачи на определенном ядре или на определенном множестве процессорных ядер. При этом задачи могут мигрировать между процессорными ядрами. В отличие от SMP, можно назначить для конкретной задачи свое процессорное ядро выполнения.

Менеджер исключений. Сообщения о каких-либо исключительных ситуациях в аппаратном обеспечении приходят в виде исключений: передачи

аппаратурой управления на заведомо определённые адреса. Исключения бывают следующих типов:

– аппаратное прерывание (генерируется устройством при наступлении заданных событий);

– исключение (некорректные действия программного кода, такие как некорректная инструкция, доступ к памяти по не выровненному адресу, ошибка виртуальной памяти);

– программное прерывание (генерируется специальной инструкцией процессора).

В задачи менеджера исключений входит обработка всех типов исключений, предоставление специального интерфейса для задания обработчиков прерываний.

Разделам предоставляется интерфейса для установки собственных обработчиков на каждый тип и источник исключения, включение или отключение прерываний. При возникновении исключения выполняется небольшая подпрограмма, выполняющая действия для сохранения текущего состояния выполнения, чтобы после обработки это состояние было восстановлена и выполнение продолжилось. Затем, менеджер определяет тип и источник исключения. Менеджер сохраняет информацию о возникшем исключении в разделе, который был сконфигурирован для получения данного типа исключений. Далее, происходит восстановление процесса выполнения. В зависимости от того, запросил ли данный раздел отключение прерываний, информация об исключений либо откладывается до включения прерываний в разделе, либо обрабатывается согласно принятым соглашениям (установка состояния раздела в специальный режим без возникновения исключений, передача управления на заведомо определённый адрес в разделе). Обработчик исключений раздела получает из сохранённой информации тип и источник исключения, откладывает вызов обработчика прерываний. Затем он переводит раздел в регулярный режим, происходит вызов отложенного обработчика.

Далее выполняется вызов установленного ранее в разделе обработчика исключений конкретного типа и источника.

Менеджер системных вызовов. Системные вызовы (программные исключения) обеспечивают механизм взаимодействия программ пользовательского пространства и подпрограмм пространства ядра. Менеджер системных вызовов предоставляет обработку системных вызовов в каждом разделе. При вызове программного прерывания особого номера в прикладной программе, менеджер исключений передаёт информацию о нём в ядро раздела. Задача менеджера состоит в том, чтобы определить поток, вызвавший прерывание, и вызвать функцию ядра, соответствующее номеру прерывания в данном потоке.

Менеджер управления памятью. За распределение памяти в системе отвечает менеджер управления памятью. Он имеет несколько уровней управления памятью. В ядре содержится модуль, отвечающий за распределение физической памяти, обычно блоками. Поверх этих блоков строятся собственные распределители памяти. Выделение памяти может происходить статически на этапе сборки образа, и динамически, в момент работы системы.

Статическое выделение памяти используется для задания областей памяти, которые известны на этапе сборки, например карта памяти устройств или задание памяти под фиксированный сегмент системы. Для статического распределения используются линкер скрипты. При таком распределении нет дополнительных расходов на распределение памяти в системе. Но имеются большие потери при ее использовании, поскольку необходимо задавать максимальную границу используемой памяти.

Динамическое распределение памяти строится поверх той или иной области заданной статически. При любом динамическом распределении памяти имеются накладные расходы на выделение каждого блока.

Основная задача ядра наряду с эффективным управлением ресурсов является изоляции защита данных различных процессов. Для защиты данных может быть использовано два метода:

– страничный;

– сегментный.

Сегментный метод (сегментная организация памяти) заключается в предоставлении различных сегментов памяти разным задачам. Адресация в этом случае идет с относительным смещением от начала сегмента. Каждый сегмент может быть защищен отдельно. Ядро занимается проверкой прав при смене сегмента.

Страничная организация памяти является более гибким механизмом. Вся память системы делится на страницы одинакового размера. Таким образом при обращении в какой-то адрес можно однозначно определить страницу (а следовательно, и ее права).

Ядро системы может использовать аппаратную поддержку защиты страниц, изоляцию пространств, а также преобразование виртуальных адресов в физические.

– Планировщик устройств есть модуль ядра системы, который занимается планированием доступа разделов к физическим устройствам.

Виды доступа к устройствам:

– совместный доступ: устройство доступно в нескольких разделах;

– раздельный доступ: устройство доступно ровно в одном разделе.

Права доступа к устройствам:

– нет прав доступа: устройство не доступно для данного раздела;

– только получение данных;

– только посылка данных;

– получение и посылка данных.

Безопасность доступа к устройствам:

– раздел не может сам изменить права доступа. Они выставляются планировщиком;

– планировщик выделяет квант времени разделу на посылку/получение при совместном доступе.

Планировщик устройств обеспечивает корректную обработку приведенных выше случаев [2].

2 Сравнительный анализ Embox с аналогичными операционными системами

На рынке существует широкий выбор ОС реального времени. Наиболее актуальными ОС реального времени являются системы:

– FreeRTOS;

– eCos.

FreeRTOS - это многозадачная, кроссплатформенная, бесплатная операционная система жесткого реального времени с открытым исходным кодом.

Основные характеристики FreeRTOS:

– планировщик FreeRTOS поддерживает три типа многозадачности:

– вытесняющую;

– кооперативную;

– гибридную.

– размер ядра FreeRTOS составляет всего 4–9 кбайт, в зависимости от типа платформы и настроек ядра;

– FreeRTOS написана на языке C (исходный код ядра представлен в виде всего лишь четырех C-файлов);

– поддерживает задачи (tasks) и сопрограммы (coroutines). Сопрограммы специально созданы для МК с малым объемом ОЗУ;

– возможность отслеживать факт переполнения стека;

– нет программных ограничений на количество одновременно выполняемых задач;

– нет программных ограничений на количество приоритетов задач;

– нет ограничений в использовании приоритетов: нескольким задачам может быть назначен одинаковый приоритет [3].

eCOS – ОС реального времени с открытым кодом, предназначена для применения во встраиваемых системах и способна работать на микроконтроллерах.

ОС eCOS предоставляет обладает следующими особенностями:

– уровень абстракции оборудования HAL;

– ядро реального времени;

– обработку прерываний и исключений;

– выбор планировщика;

– поддержку многопоточности и примитивов синхронизации;

– таймеры, счётчики;

– механизмы управления памятью;

– отладку посредством GDB;

– набор библиотек;

– драйверы различных устройств;

– поддержку файловых систем.

Проведено сравнение упомянутых ОС по ключевым параметрам.

Каждая из операционных систем поддерживает большое количество архитектур общими их которых являются:

– ARM (ARM7, ARM9, StrongARM, XScale, Cortex-M);

– x86;

– MIPS;

– Microblaze;

– SPARC;

– PPC.

Наиболее широким набором поддерживаемых архитектур обладает система eCos, что позволяет ей быть наиболее востребованной на рынке за счет возможности ее интеграции в большую часть аппаратных средств.

Система FreeRTOS также обладает большим количеством архитектур, но уступает в этом компоненте eCos.

Embox обладает меньшим набором архитектур, но для решения задач, которые перед ней ставятся существующего набора более чем достаточно.

ОС embox – имеет лицензию BSD (свободно распространяемое программное обеспечение), с открытым исходным кодом, что позволяет

разработчикам, использующим данную ОС, вносить в код коррективы необходимые для выполнения поставленных перед ними задач. В отличии от embox системы eCos и FreeRTOS являются не только свободными, но и коммерческими.

В ОС FreeRTOS существуют так называемые официально поддерживаемые аппаратные платформы - официальные порты и неофициальные, которые поставляются «как есть» и не поддерживаются напрямую. Примером коммерческих версий являются: SafeRTOS и OpenRTOS. SafeRTOS — это ОС РВ, имеющая такую же функциональную модель, что и FreeRTOS, ориентированная на применение в системах с высокими требованиями к безопасности, например, в медицинской и аэрокосмической отраслях.

eCos реализована на языке C. Задачи для данной ОС могут быть реализованы на языке C++.

FreeRTOS выполнена на языке C. Для оптимизации работы на определенной платформе могут быть использованы вставки написанные на ассемблере.

Embox также, как и FreeRTOS реализована на языке C, с использованием вставок написанных на ассемблере.

В языке C существует проблема переполнения стека. Так как дополнительное ПО разрабатывается на языке C в ОС интегрированы механизмы отслеживания переполнений.

Для решения этой проблемы в embox реализованы менеджер управления памятью, а также планировщик распределения системных ресурсов.

Ключевым преимуществом embox над eCos и FreeRTOS является полная модульность – при необходимости можно создать образ ядра системы обладающей классическим менеджером ресурсов (диспетчер памяти, потоков и.т.д), можно создать образ, запускающий определенный поток по определенному событию, что уменьшит накладные расходы на планирование задач. Или, создать образ, позволяющий привязывать задачу к каким-то

ресурсам системы, процессорному ядру, области памяти и т.д. Такие свойства ОС Embox достигаются за счет возможности задать различные реализации системных диспетчеров ресурсов.

В то время, как ОС eCos и FreeRTOS также являются модульными системами, но в отличии от embox ядро каждой из систем является сформированным на этапе разработки.

Еще одним преимуществом является не зависимость системы от планировщика, что позволяет наиболее оптимально распределять вычислительные ресурсы.

Также преимуществом embox является наличие русскоязычной документации, находящейся в открытом доступе.

3 Оценка рисков

3.1 Идентификация среды использования операционной системы embox

Операционная система embox является встраиваемой ОС - данные системы предназначены для управления специализированными устройствами и вследствие этого способные работать в условиях ограниченных ресурсов.

Объектом исследования является отдел организации, занимающийся тестированием программного обеспечения. Для обеспечения информационной безопасности отдела используются специализированные программно-аппаратные комплексы (ПАК). В состав ПАК входит программное обеспечение, а также плата с предустановленной ОС embox.

3.2 Идентификация активов, угроз ИБ, уязвимостей активов, сценариев инцидентов ИБ

3.2.1 Идентификация информационных активов

Для идентификации информационных активов отдела тестирования осуществлено проектирование схемы бизнес процессов. Результат проектирования представлен на рисунке 2.

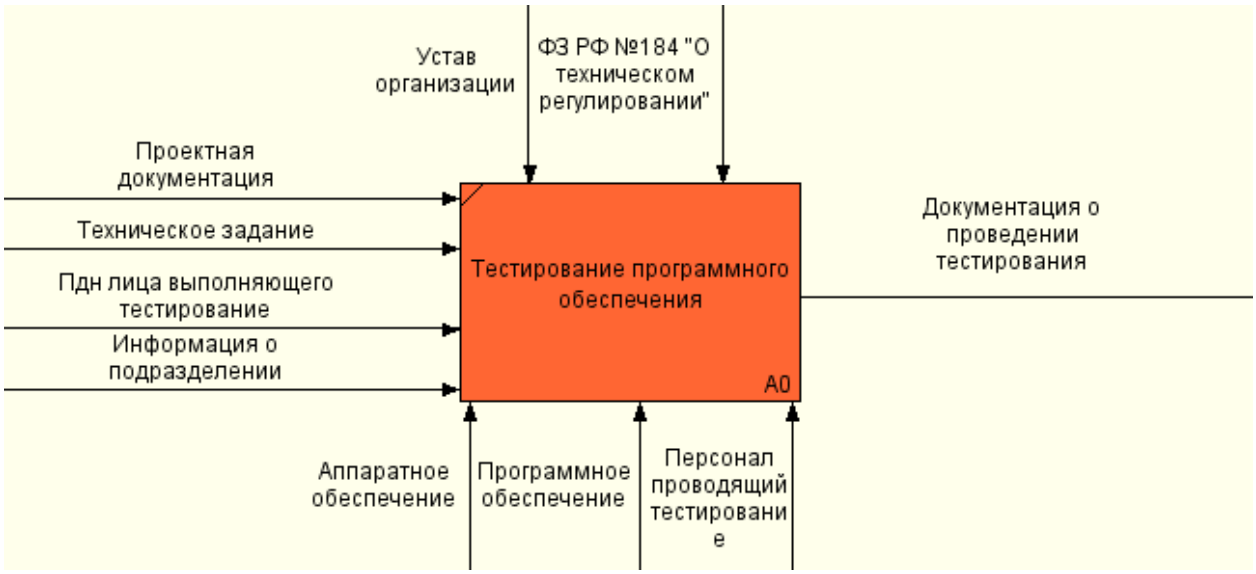

Рисунок 2 – Схема бизнес процесса

На основе схемы бизнес-процесса отдела тестирования, идентифицированы информационные активы отдела, произведена оценка основных свойств ИБ данных активов. Результат представлен в таблице 1.

Таблица 1 – Основные информационные активы отдела тестирования

Информационный актив	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
Код исследуемой программы (ИА1)	+	+	+
Техническое задание (ИА2)	+	+	+
Информация о подразделении (ИА3)	-	+	-
Пдн лица выполняющего тестирования (ИА4)	+	+	–

После составления перечня информационных активов и определения значимости их свойств проведена оценка величин ущерба от нарушения свойств ИБ активов по следующим направлениям:

– степень влияния на непрерывность деятельности организации;

– объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;

– объем дополнительных людских ресурсов, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;

– объем дополнительных временных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ;

– степень нарушения законодательных требований и(или) договорных обязательств организации.

На основании результатов оценивания величины нарушений ИБ для каждого информационного актива была определена обобщенная качественная оценка величины нарушения ИБ. Результат выполнения представлен в таблице 2.

Таблица 2 – Результат оценки величины нарушения

Информационный актив	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщенная величина нарушения ИБ	Ценности актива
		1	2	3	4	5		
Код исследуемой программы (ИА1)	Конфиденциальность	В	С	В	С	В	В	В
	Целостность	В	В	С	С	В	С	
	Доступность	В	С	С	С	В	В	
Техническое задание (ИА2)	Конфиденциальность	С	С	С	С	М	С	С
	Целостность	В	С	С	С	С	С	
	Доступность	М	М	С	С	М	М	
Информация о подразделении (ИА3)	Конфиденциальность	М	С	С	С	В	С	С
	Целостность	С	С	С	В	С	С	
	Доступность	М	С	С	В	В	С	
Пдн лица выполняющего тестирования (ИА4)	Конфиденциальность	М	С	В	С	В	С	В
	Целостность	С	С	В	С	В	С	
	Доступность	С	С	В	С	В	С	

После того, как была проведена оценка величины нарушения ИБ выполнена идентификация вспомогательных активов и зависимости между ними и основными активами организации. Результат выполнения представлен в виде матрицы зависимостей оформленной в таблицу 3.

Таблица 3 - Матрица зависимостей между активами организации

Актив / зависимый актив	АО (ВА1)	ПО (ВА2)	База данных (ВА3)	Разработчик(ВА4)
Код исследуемой программы (ИА1)	+	+	+	+
Техническое задание (ИА2)	+	+	+	+

Продолжение таблицы 3

Актив зависимый актив	АО (ВА1)	ПО (ВА2)	База данных (ВА3)	Разработчик(ВА4)
Информация о подразделении (ИА3)	-	-	+	-
Пдн лица выполняющего тестирования (ИА4)	–	+	+	+

Произведена оценка ценности вспомогательных активов. Результат выполнения представлен в таблице 4.

Таблица 4 – Оценка ценности вспомогательных активов

Актив	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива
		Актив	Ценность	
АО	В	Код исследуемой программы	В	В
		Техническое задание	В	
ПО	С	Код исследуемой программы	В	С
		Техническое задание	В	
		Пдн лица выполняющего тестирования	С	

Продолжение таблицы 4

Актив	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива
		Актив	Ценность	
Банк данных	С	Код исследуемой программы	В	С
		Техническое задание	В	
		Информация о подразделении	С	
		Пдн лица выполняющего тестирования	С	
Разработчик	В	Код исследуемой программы (ИА1)	В	В
		Техническое задание (ИА2)	В	
		Пдн лица выполняющего тестирования	С	

3.2.2 Идентификация угроз информационной безопасности

Произведена идентификация угроз ИБ организации, определены источники угроз (кто и что является причиной угрозы), установлены цели угроз (то есть, на какие активы может оказать влияние угроза) и типы потерь (то есть, на нарушение каких свойств ИБ угроза может быть направлена) [5]. Результат выполнения представлен в таблице 5.

Таблица 5 – Идентификация угроз информационной безопасности

№	Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
1	Нарушение энергоснабжения	С, У, П	Инсайдеры	ВА1, ВА2 ИА1, ИА2, ИА3	Доступность

Продолжение таблицы 5

№	Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
2	Отказ телекоммуникационного оборудования	С, У	Лицо, совершающее компьютерное преступление	ВА1, ВА2, ВА3 ИА1, ИА2	Доступность
3	Преступное использование аппаратных средств	У	Инсайдеры	ВА1, ВА3 ИА1, ИА2, ИА3	Целостность
4	Нарушение функционирования программного обеспечения	С,У	Инсайдеры	ВА2, ВА3 ИА1, ИА2	Доступность
5	Включение в проект не достоверно испытанных компонентов	У	Лицо, совершающее компьютерное преступление	ВА1 ИА1	Конфиденциальность
6	Угроза доступа к защищаемым файлам с использованием обходного пути	У	Лицо, совершающее компьютерное преступление	ВА3 ИА1, ИА2, ИА3	Целостность
7	Злоупотребление правами	У	Инсайдеры	ИА1, ИА2, ИА3, ИА4	Конфиденциальность
8	Искажение информации, хранящейся в БД	У	Лицо, совершающее компьютерное преступление	ВА3, ВА4 ИА3	Целостность
9	Внедрение вредоносного ПО	У	Лицо, совершающее компьютерное преступление	ВА2, ВА3 ИА1, ИА2	Доступность

Продолжение таблицы 5

№	Угроза	Тип событий	Источник угрозы	Цель угрозы	Тип потери
10	Несанкционированное использование ПО	У	Лицо, совершающее компьютерное преступление	ВА2, ИА1, ИА2	Целостность
11	Несанкционированный доступ к информации, хранящейся в БД	У	Лицо, совершающее компьютерное преступление	ИА1, ИА2, ИА3 ВА3, ВА4	Конфиденциальность

Где типы событий:

- С – случайные;
- У – умышленные;
- П – природные.

3.2.3 Идентификация уязвимостей активов информационной системы

Для каждого актива идентифицированы уязвимости. Кроме того, были учтены уязвимости вспомогательных активов, обеспечивающих хранение, обработку, передачу основных активов, поскольку использование уязвимостей аппаратных средств, ПО, персонала и.т.д., может повлечь нарушение свойств ИБ основных активов [5].

– УЯ 1 – слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов;

– УЯ 2 - уязвимость, внедряемая автоматизированными средствами проектирования/разработки;

– УЯ 3 - недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью;

– УЯ 4 - ошибки в настройке системы разграничения доступа к объектам файловой системы;

– УЯ 5 – возможность выхода из строя критически важного модуля;

– УЯ 6 – отсутствие контроля изменений конфигураций аппаратного и программного обеспечения;

– УЯ 7 – отсутствие политик использования телекоммуникационной среды и обмена сообщениями;

– УЯ 8 – отсутствие регулярных аудитов;

– УЯ 9 – отсутствие надлежащего распределения обязанностей по обеспечению ИБ;

– УЯ 10 – недостаточное техническое обслуживание.

Результат выполнения представлен в таблице 6.

Таблица 6 – Идентификация уязвимости

Актив	Уязвимости	Связанные уязвимости
Вспомогательные		
АО (ВА1)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1); уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2); возможность выхода из строя критически важного модуля (УЯ5)	
ПО (ВА2)	уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2); ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4; недостаточное техническое обслуживание (УЯ10)	

Продолжение таблицы 6

Актив	Уязвимости	Связанные уязвимости
Вспомогательные		
База данных (ВА3)	уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2); недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью (УЯ3); ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	
Разработчик(ВА4)	отсутствие политик использования телекоммуникационной среды и обмена сообщениями (УЯ7); отсутствие надлежащего распределения обязанностей по обеспечению ИБ (УЯ9).	
Основные		
Код исследуемой программы (ИА1)	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4); возможность выхода из строя критически важного модуля (УЯ5); отсутствие политик использования телекоммуникационной среды и обмена сообщениями (УЯ7)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1); отсутствие надлежащего распределения обязанностей по обеспечению ИБ (УЯ9).

Продолжение таблицы 6

Актив	Уязвимости	Связанные уязвимости
Основные		
Техническое задание (ИА2)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1); уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2); отсутствие контроля изменений конфигураций аппаратного и программного обеспечения (УЯ6).	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4); возможность выхода из строя критически важного модуля (УЯ5); отсутствие регулярных аудитов (УЯ8).
Информация о подразделении (ИА3)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1); уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2).	отсутствие регулярных аудитов (УЯ8); недостаточное техническое обслуживание (УЯ10)
Пдн лица выполняющего тестирования (ИА4)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1); ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4); телекоммуникационной среды и обмена сообщениями (УЯ7)	отсутствие регулярных аудитов (УЯ8); недостаточное техническое обслуживание (УЯ10)

3.2.4 Идентификация существующих защитных мер

В рассматриваемой организации существуют следующие защитные меры:

– разграничение доступа к файлам стандартными средствами администрирования, встроенными в ОС;

– организован пропускной режим по подразделениям организации;

– сформирован «черный список программного обеспечения»;

– установлены антивирусы (устаревшие версии);

– на маршрутизаторах сформированы листы ACL (access control list).

Данных защитных мер недостаточно для безопасной обработки секретной информации, либо конфиденциальной информации.

3.2.5 Идентификация последствий

Последствие - результат события, оказывающего влияние на цели.

Целью данного этапа является определение последствий (ущерба) для отдела организации, которые могут быть обусловлены сценариями возможных инцидентов. Сценарий инцидента является описанием угрозы, использующей определенную уязвимость или набор уязвимостей актива во время инцидента ИБ.

Связи между угрозами, уязвимостями активов, которые могут быть использованы для их реализации, и активами представлены в виде таблицы. Для каждого сценария идентифицированы его последствия.

Результатом процесса является перечень сценариев инцидентов с их последствиями, связанными с активами. Результат выполнения представлен в таблице 7.

Таблица 7 – Сценарии инцидентов

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Нарушение энергоснабжения (У1)	недостаточное техническое обслуживание (УЯ10)	ВА2, ИА3	Нарушение доступности ИА3	Потери время на восстановление
		ИА4	Нарушение доступности ИА4	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Нарушение энергоснабжения (У1	отсутствие надлежащего распределения обязанностей по обеспечению ИБ (УЯ9)	ИА1	Нарушение доступности ИА1	Потери время на восстановление
		ВА4	Нарушение доступности ВА4	Потери время на восстановление
Отказ телекоммуникационного оборудования (У2)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1)	ВА1, ВА3, ИА2	Нарушение целостности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА1, ВА1, ВА2	Нарушение доступности ИА1	Потери время на восстановление
	уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2)	ВА1, ИА1	Нарушение целостности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ВА2, ИА2 ВА3	Нарушение доступности ИА2	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
	отсутствие контроля изменений конфигураций аппаратного и программного обеспечения (УЯ6)	ВА1, ВА2, ВА3, ИА1	Нарушение доступности ИА1	Потери время на восстановление
		ВА1, ВА2, ВА3, ИА2	Нарушение доступности ИА2	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Преступное использование аппаратных средств (У3)	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	ИА1, ВА1, ВА2	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА1, ВА2	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА3, ВА1	Нарушение доступности ИА3	Потери время на восстановление
	отсутствие политик использования телекоммуникационной среды и обмена сообщениями (УЯ7)	ИА1, ВА2	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2, ВА1, ВА2	Нарушение целостности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3, ВА1	Нарушение доступности ИА3	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
		ИА3, ВА1	Нарушение доступности ИА3	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Преступное использование аппаратных средств (У3)	отсутствие регулярных аудитов (УЯ8)	ИА1, ВА1, ВА2	Нарушение целостность ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2, ВА1	Нарушение доступности ИА2	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
		ИА3, ВА1	Нарушение доступности ИА3	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
Нарушение функционирования программного обеспечения (У4)	недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью (УЯ3)	ИА2, ВА1	Нарушение доступности ИА2	Потери время на восстановление
		ИА1, ВА2	Нарушение доступности ИА1	Потери время на восстановление
	уязвимость, внедряемая автоматизированными средствами проектирования/разработки (УЯ2)	ИА1, ВА1, ВА2	Нарушение доступности ИА1	Потери время на восстановление
		ИА2, ВА1	Нарушение доступности ИА2	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Включение в проект не достоверно испытанных компонентов (У5)	недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью (УЯ3)	ИА1, ВА1	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
	возможность выхода из строя критически важного модуля (УЯ5)	ИА1, ВА1	Нарушение доступности ИА1	Потери время на восстановление
Угроза доступа к защищаемым файлам с использованием обходного пути (У6)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1)	ИА1	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2	Нарушение конфиденциальности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3, ВА3	Нарушение конфиденциальности ИА3	Потеря репутации, вследствие нарушения законодательных требований
	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	ИА1	Нарушение доступности ИА1	Потери время на восстановление
		ИА2, ВА3	Нарушение доступности ИА2	Потери время на восстановление
		ИА3	Нарушение доступности ИА3	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Угроза доступа к защищаемым файлам с использованием обходного пути (У6)	отсутствие контроля изменений конфигураций аппаратного и программного обеспечения (УЯ6)	ИА1, ВА3	Нарушение целостности ИА1	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
		ИА2	Нарушение целостности ИА2	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
		ИА3	Нарушение целостности ИА1	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
Злоупотребление правами (У7)	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	ИА1	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2	Нарушение конфиденциальности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3	Нарушение конфиденциальности ИА3	Потери время на восстановление
		ИА4	Нарушение конфиденциальности ИА4	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Злоупотребление правами (У7)	отсутствие надлежащего распределения обязанностей по обеспечению ИБ (УЯ9)	ИА1	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2	Нарушение конфиденциальности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3	Нарушение конфиденциальности ИА3	Потери время на восстановление
		ИА4	Нарушение конфиденциальности ИА4	Потери время на восстановление
Искажение информации, хранящейся в БД (У8)	отсутствие регулярных аудитов (УЯ8)	ИА3, ВА3, ВА4	Нарушение целостности ИА3	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива
Внедрение вредоносного ПО (У9)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1)	ИА1, ВА2	Нарушение целостности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2, ВА3	Нарушение доступности ИА2	Потери время на восстановление
	отсутствие контроля изменений конфигураций аппаратного и программного обеспечения (УЯ6)	ИА1, ВА2, ВА3	Нарушение целостности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2	Нарушение доступности ИА2	Потери время на восстановление

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Несанкционированное использование ПО (У10)	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	ИА1, ВА 2	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2	Нарушение конфиденциальности ИА2	Потеря репутации, вследствие нарушения законодательных требований
	отсутствие контроля изменений конфигураций аппаратного и программного обеспечения (УЯ6)	ИА1	Нарушение доступности ИА1	Потери время на восстановление
		ИА2, ВА2	Нарушение доступности ИА2	Потери время на восстановление
Несанкционированный доступ к информации, хранящейся в БД (У11)	слабость сетевых протоколов, ошибки, допущенные в ходе реализации протоколов (УЯ1)	ИА1	Нарушение целостности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2, ВА3	Нарушение целостности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3, ВА3, ВА4	Нарушение доступности ИА3	Финансовые затраты, связанные, со стоимостью восстановления резервной копии актива

Продолжение таблицы 7

Угроза	Уязвимости, необходимые для реализации угрозы	Затрагиваемые активы	Событие	Последствия
Несанкционированный доступ к информации, хранящейся в БД (У11)	ошибки в настройке системы разграничения доступа к объектам файловой системы (УЯ4)	ИА1	Нарушение конфиденциальности ИА1	Потеря репутации, вследствие нарушения законодательных требований
		ИА2, ВА3	Нарушение конфиденциальности ИА2	Потеря репутации, вследствие нарушения законодательных требований
		ИА3, ВА3, ВА4	Нарушение конфиденциальности ИА3	Потеря репутации, вследствие нарушения законодательных требований

4 Анализ и оценивание риска информационной безопасности

4.1 Анализ риска

Целью данного этапа является определение уровня риска для всех значимых сценариев инцидентов.

Уровень риска - величина риска, выраженная с точки зрения комбинации последствий и их вероятности.

Для определения уровня рисков были оценены вероятности инцидентов, как сочетания возможностей реализации угроз (возможности угроз) и оценок возможностей использования уязвимостей (уровни уязвимостей) [6]. Возможность угрозы и уровни уязвимости могут иметь значения:

– В – высокий уровень;

– С – средний уровень;

– Н – низкий уровень.

Шкала оценки вероятности сценария инцидента произведена в соответствии с таблицей 8.

Таблица 8 – Шкала оценивания

Возможность угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Возможность сценария инцидента	0	1	2	1	2	3	2	3	4

Результаты определения вероятностей инцидентов представлены в таблице 9.

Таблица 9 – Определение вероятности инцидентов

Инцидент	Угроза	Возможность угрозы	Уязвимость	Уровень уязвимости	Вероятность сценария инцидента
ИН1	У1	Средняя	УЯ10	С	2
ИН2			УЯ9	Н	1
ИН3	У2	Низкая	УЯ1	Н	0
ИН4			УЯ2	С	1
ИН5			УЯ6	С	1
ИН6	У3	Средняя	УЯ4	В	3
ИН7			УЯ7	В	3
ИН8			УЯ8	С	2
ИН9	У4	Средняя	УЯ3	С	2
ИН10			УЯ2	Н	1
ИН11	У5	Низкая	УЯ3	Н	0
ИН12			УЯ5	С	1

Продолжение таблицы 9

Инцидент	Угроза	Возможность угрозы	Уязвимость	Уровень уязвимости	Вероятность сценария инцидента
ИН13	У6	Средняя	УЯ1	С	2
ИН14			УЯ4	В	3
ИН15			УЯ6	С	2
ИН16	У7	Высокая	УЯ4	С	3
ИН17			УЯ9	В	4
ИН18	У8	Низкая	УЯ8	Н	1
ИН19	У9	Средняя	УЯ1	Н	1
ИН20			УЯ6	С	2
ИН21	У10	Средняя	УЯ4	В	3
ИН22			УЯ6	С	2
ИН23	У11	Низкая	УЯ1	Н	0
ИН24			УЯ4	С	1

4.2 Оценивание риска

Произведено определение уровня риска методом ранжирования угроз мерами риска. Данный метод связывает ценность активов с вероятностью возникновения угрозы (принимая в расчет аспекты уязвимости).

В качестве шкалы оценивания последствий используются числа в диапазоне от 1 до 3.

Меры риска вычисляются путем умножения значений столбца ценность актива, на значение столбца возможность возникновения угрозы. В результате, угрозы ранжированы в соответствии с их мерами риска [5]. Результат выполнения представлен в таблице 10.

Таблица 10 - Определение уровня риска

Идентификатор угрозы	Идентификатор уязвимости(ей)	Последствия (ценность актива)	Возможность возникновения угрозы	Мера риска	Ранжирование угроз	Идентификатор сценария
У1	УЯ10	3	2	6	4	СИ1
	УЯ9	3	1	4	3	СИ2
У2	УЯ1	3	0	0	5	СИ3
	УЯ2	3	1	3	4	СИ4
	УЯ6	3	1	3	3	СИ5
У3	УЯ4	3	3	9	2	СИ6
	УЯ7	3	3	9	1	СИ7
	УЯ8	3	2	6	3	СИ8
У4	УЯ3	3	2	6	4	СИ9
	УЯ2	3	1	3	4	СИ10
У5	УЯ3	3	0	0	5	СИ11
	УЯ5	3	1	3	2	СИ12
У6	УЯ1	3	2	6	3	СИ13
	УЯ4	3	3	9	2	СИ14
	УЯ6	3	2	6	2	СИ15
У7	УЯ4	3	3	9	1	СИ16
	УЯ9	3	4	12	3	СИ17
У8	УЯ8	3	1	3	2	СИ18
У9	УЯ1	3	1	3	3	СИ19
	УЯ6	3	2	6	1	СИ20
У10	УЯ4	3	3	9	2	СИ21
	УЯ6	3	2	6	3	СИ22
У11	УЯ1	3	0	0	5	СИ23
	УЯ4	3	1	3	1	СИ24

По результатам определения уровня рисков принято решение о очередности обработки угроз. В первую очередь необходимо уделить особое внимание угрозам с рангом 1-2 (высокий риск) включительно, затем угрозам с рангом 3 (средний риск) включительно и в последнюю очередь угрозам с рангом 4-5 включительно.

4.3 Выбор защитных мер в заданных областях обеспечения информационной безопасности

4.3.1 Определение способов обработки рисков информационной безопасности

Существуют следующие способы обработки рисков ИБ:

– предотвращение риска — решение не быть вовлечённым в рискованную ситуацию или действие, предупреждающее вовлечение в неё;

– снижение риска — действие, предпринятое для уменьшения вероятности негативных последствий или того и другого вместе, связанных с риском;

– перенос риска — разделение с другой стороной бремени потерь или выгод от риска.

Для всех информационных и вспомогательных активов был определён способ обработки риска. Результат представлен в таблице 11.

Таблица 11 – Выбор способов обработки рисков

Актив	Сценарий	Способ обработки
ИА1	СИ1	Перенос
	СИ2	Снижение
	СИ4	Снижение
	СИ5	Снижение
	СИ6	Снижение
	СИ7	Снижение
	СИ8	Снижение
	СИ9	Перенос
	СИ10	Перенос
	СИ11	Принятие
	СИ12	Снижение
	СИ13	Снижение
	СИ14	Снижение
	СИ15	Снижение
	СИ16	Снижение

Продолжение таблицы 11

Актив	Сценарий	Способ обработки
	СИ17	Снижение
	СИ19	Перенос
	СИ20	Перенос
	СИ21	Снижение
	СИ22	Снижение
	СИ23	Принятие
	СИ24	Снижение
ИА2	СИ1	Перенос
	СИ2	Снижение
	СИ3	Принятие
	СИ4	Перенос
	СИ5	Снижение
	СИ6	Снижение
	СИ7	Перенос
	СИ8	Перенос
	СИ9	Принятие
	СИ10	Перенос
	СИ13	Перенос
	СИ14	Снижение
	СИ15	Снижение
	СИ16	Снижение
	СИ17	Снижение
	СИ19	Снижение
	СИ20	Перенос
	СИ21	Снижение
	СИ22	Перенос
	СИ23	Принятие
	СИ24	Снижение

Продолжение таблицы 11

Актив	Сценарий	Способ обработки
ИА3	СИ1	Перенос
	СИ6	Снижение
	СИ8	Перенос
	СИ13	Перенос
	СИ14	Снижение
	СИ16	Снижение
	СИ17	Снижение
	СИ23	Принятие
	СИ24	Снижение
ИА4	СИ16	Снижение
	СИ17	Перенос
ВА1	СИ2	Перенос
	СИ4	Перенос
	СИ5	Снижение
	СИ6	Снижение
	СИ7	Снижение
	СИ8	Перенос
	СИ11	Принятие
	СИ12	Снижение
ВА2	СИ1	Перенос
	СИ2	Перенос
	СИ4	Перенос
	СИ5	Снижение
	СИ9	Принятие
	СИ10	Принятие
	СИ19	Перенос
	СИ20	Снижение
	СИ23	Принятие

Продолжение таблицы 11

Актив	Сценарий	Способ обработки
ВА3	СИ4	Перенос
	СИ5	Снижение
	СИ6	Снижение
	СИ7	Снижение
	СИ8	Снижение
	СИ9	Снижение
	СИ10	Принятие
	СИ13	Перенос
	СИ14	Снижение
	СИ15	Снижение
	СИ18	Снижение
	СИ19	Перенос
	СИ20	Снижение
	СИ23	Принятие
	СИ24	Снижение
ВА4	СИ18	Принятие
	СИ23	Принятие
	СИ24	Снижение

4.3.2 Выбор защитных мер

С целью снижения риска ИБ до приемлемого уровня определены требования к защитным мерам. В соответствии с выбранным способом обработки рисков для каждого актива должны быть определены требования к защитным мерам для снижения уровня уязвимости или противодействия реализации угрозы, а также варианты их реализации в виде технических (аппаратных, программно-аппаратных или программных) средств (ТС) или организационных мер (ОМ) (например, инструкции для персонала, регламенты, положения, политики)

Области, в которых могут быть применены защитные меры в соответствии с ГОСТ Р ИСО/МЭК 27002-2012 [7]:

– управление активами;

– информационная безопасность, связанная с персоналом;

– физическая защита и защита от воздействия окружающей среды;

– управление передачей данных и операционной деятельностью;

– контроль доступа;

– разработка и обслуживание систем;

– обработка инцидентов информационной безопасности;

– управление непрерывностью бизнеса.

Результаты представлены в таблице 12.

Таблица 13 – Защитные меры

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Приобретение, разработка и эксплуатация информационных систем.	Формулировки деловых требований для новых информационных систем, или улучшения существующих информационных систем Должны специфицировать требования для средств управления защитой.	ЗМ1
	Должна осуществляться валидация данных, вводимых в приложения, с целью гарантировать, что эти данные являются правильными и уместными.	ЗМ2
	В приложения должны быть встроены валидационные проверки, с целью предотвратить любую порчу информации вследствие ошибок обработки или умышленных действий.	ЗМ3
	Должны быть определены требования к обеспечению аутентичности и защите целостности сообщений в приложениях, и должны Быть определены и реализованы соответствующие средства управления.	ЗМ4
	Должна быть разработана и реализована политика по использованию криптографических средств управления для защиты информации.	ЗМ5
	Для поддержки использования организацией криптографических методов должно иметься распределение ключей.	ЗМ6

Продолжение таблицы 12

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Приобретение, разработка и эксплуатация информационных систем.	Должны быть приняты процедуры для управления установкой программного обеспечения в операционных системах.	ЗМ7
	Испытательные данные должны выбираться тщательно, и должны быть защищены и управляемы.	ЗМ8
	Доступ к исходному коду программы должен быть ограничен.	ЗМ9
	При смене операционной системы, деловые критические приложения должны анализироваться и испытываться, с целью гарантировать отсутствие неблагоприятного влияния на организационные операции или защиту.	ЗМ10
	Необходимо препятствовать модификациям в пакетах программ, эти модификации должны быть ограничены необходимыми изменениями, и все изменения должны строго контролироваться.	ЗМ11
	Возможности для утечки информации должны предупреждаться.	ЗМ12
	Должна быть получена своевременная информация о технических слабых местах используемых информационных систем, оценена подверженность организации влиянию таких слабых мест, и предприняты подходящие меры для того, чтобы учесть связанный с ними риск.	ЗМ13
Менеджмент непрерывности бизнеса	Необходимо разрабатывать и поддерживать управляемый процесс для обеспечения непрерывности бизнеса во всей организации, который учитывает требования к информационной безопасности, необходимые для обеспечения непрерывности бизнеса организации.	ЗМ14
	События, которые могут стать причиной прерываний процессов бизнеса, необходимо определять вместе с вероятностью и влиянием таких прерываний, а также их последствиями для информационной безопасности.	ЗМ15
	Необходимо разработать и внедрить планы обеспечения непрерывности бизнеса с целью поддержки или восстановления операций и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или сбоя критических процессов бизнеса.	ЗМ16

Продолжение таблицы 12

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Менеджмент непрерывности бизнеса	Следует поддерживать единую структуру планов непрерывности бизнеса, чтобы обеспечить уверенность в том, что все планы согласованы в соответствии с рассматриваемыми требованиями информационной безопасности и установленными приоритетами для тестирования и обслуживания.	ЗМ17
	Планы непрерывности бизнеса необходимо регулярно тестировать и обновлять с целью обеспечения уверенности в их актуальности и эффективности.	ЗМ18
Менеджмент коммуникаций и работ	Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.	ЗМ19
	Изменения в конфигурации средств обработки информации и системах должны контролироваться.	ЗМ20
	Обязанности и области ответственности должны быть разделены для уменьшения возможностей неавторизованной или непреднамеренной модификации активов организации или их нецелевого использования.	ЗМ21
	Чтобы снизить риски неавторизованного доступа или изменений эксплуатируемой системы, следует обеспечивать разделение средств разработки, тестирования и эксплуатации.	ЗМ22
	Необходимо регулярно проводить мониторинг и анализ услуг, отчетов и записей, обеспечиваемых третьей стороной, и регулярно проводить аудиты.	ЗМ23
	Изменения в предоставлении услуг, включая поддержку и улучшение существующих политик, процедур, мер и средств контроля и управления информационной безопасности, должны осуществляться с учетом критичности затрагиваемых систем и процессов бизнеса, а также переоценки рисков.	ЗМ24
	Использование ресурсов необходимо прогнозировать, исходя из будущих требований к производительности, настраивать и контролировать, чтобы обеспечить уверенность в достижении требуемых экспл. данных системы.	ЗМ25

Продолжение таблицы 12

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Менеджмент коммуникаций и работ	Должны быть определены критерии приемки для новых информационных систем, обновлений и новых версий, кроме того, необходимо тестировать системы в течение их разработки и перед их приемкой.	ЗМ26
	Необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей	ЗМ27
	Сети должны адекватно управляться и контролироваться, чтобы быть защищенными от угроз и обеспечить безопасность систем и прикладных программ, использующих сеть, включая информацию во время ее передачи.	ЗМ28
	Средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента всех сетевых услуг должны быть определены и включены в любой договор по сетевым услугам, вне зависимости от того, будут ли они обеспечиваться силами организации или в рамках договоров аутсорсинга.	ЗМ29
	Должны существовать процедуры в отношении менеджмента сменных носителей информации.	ЗМ30
	Носители информации, когда в них больше нет необходимости, следует надежно и безопасно утилизировать, используя формальные процедуры.	ЗМ31
	С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации.	ЗМ32
	Системная документация должна быть защищена от неавторизованного доступа.	ЗМ33
	Должны существовать формальные политики, процедуры и меры и средства контроля и управления в отношении обмена информацией с целью защиты такого обмена, когда используются все типы средств связи.	ЗМ34

Продолжение таблицы 12

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Менеджмент коммуникаций и работ	Носители информации должны быть защищены от неавторизованного доступа, неправильного использования или повреждения во время их транспортировки за пределами организации.	ЗМ35
	Необходимо должным образом защищать информацию, включаемую в электронный обмен сообщениями.	ЗМ36
	Необходимо разработать и внедрить политики и процедуры защиты информации, связанной с взаимодействием информационных систем бизнеса.	ЗМ73
	Целостность информации, которая доступна в общедоступной системе, следует защищать для предотвращения неавторизованной модификации	ЗМ38
	Необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом	ЗМ39
	Неисправности следует регистрировать, анализировать, и предпринимать в их отношении необходимые действия.	ЗМ40
	Часы во всех соответствующих системах обработки информации в пределах организации или домена безопасности должны быть синхронизированы с установленным источником точного времени.	ЗМ41
Менеджмент управления доступом	Необходимо создать политики распространения информации и выдачи разрешения, (например, принцип необходимого знания, уровни защиты и классификация информации)	ЗМ42
	Необходимо согласовывать управление доступом и политику в области классификации информации разных систем и сетей	ЗМ43
	Использование уникальных идентификаторов пользователей для того, чтобы дать пользователям возможность быть связанными со своими действиями и нести за них ответственность;	ЗМ44

Продолжение таблицы 12

Область обеспечения ИБ	Формулировка меры	Идентификатор меры
Менеджмент управления доступом	Проверка того, что уровень предоставленного доступа соответствует деловой цели и согласуется с организационной политикой в области защиты	ЗМ45
	Немедленное удаление или блокировка прав доступа пользователей, которые изменили роли или должности, или ушли из организации	ЗМ46
	Права доступа пользователей должны анализироваться регулярно, каждые 3 месяца, и после любых изменений, например, повышение в должности, понижение в должности или прекращение работы по найму	ЗМ47
	Распределения привилегий должно проверяться регулярно для того, чтобы обеспечить, что не были получены неразрешенные привилегии	ЗМ48
	Необходимо формирование политик для средств, применяющихся при доступе к сетям и сетевым услугам	ЗМ49

Далее разработаны организационные меры, позволяющие уменьшить вероятность реализации угрозы информационной системе при помощи, соответствующей ей уязвимости.

Список организационных мер представлен в таблице 13.

Таблица 13 – Организационные меры

Описание	Идентификатор меры
Для каждого носителя информации (бумажного или электронного) составление списка лиц, допущенных к нему	ОМ1
Ограничение доступа к информации, хранящейся на компьютерах	ОМ2
Составление списка лиц, допущенных к системной документации	ОМ3
Разработка процедуры хранения системной документации и съёмных носителей информации.	ОМ4
Разработка журнала учёта съёмных носителей информации	ОМ5
Разработка перечня обязанностей для каждого сотрудника	ОМ6
Резервное копирование информации и конфигураций с сервера БД необходимо проводить 2 раза в месяц	ОМ7
Внедрение механизма контроля целостности	ОМ8
Осуществлять обновление антивирусных баз	ОМ9
Применение механизма контроля целостности	ОМ10
Осуществлять проверку обновления антивирусных баз 1 раз в 3 дня	ОМ11

Продолжение таблицы 13

Описание	Идентификатор меры
Осуществлять сканирование компьютеров на наличие вирусов 1 раз в 3 дня	ОМ12
Наблюдение за деятельностью персонала там, где это разрешено законом	ОМ13
Опечатывание системных блоков и корпусов других технических устройств	ОМ14
Заключение договора с компанией, проводящей исследования на наличие аппаратных закладок. Частота исследований – 1 раз в 6 месяцев	ОМ15
Аудит всех действий пользователей и администраторов	ОМ16
Хранение журналов регистрации события осуществлять в течение 2-х месяцев.	ОМ17
Назначение ответственного за сеть организации	ОМ18
Разработка и ведение журнала учёта неисправностей	ОМ19
Разработка и внедрение планов непрерывности бизнеса	ОМ20
Составление списка лиц для выдачи им электронных ключей	ОМ21
Ведение журнала выдачи электронных ключей	ОМ22

Также для обеспечения информационной безопасности необходимо использование технических средств (ТС), предназначенных для уменьшения вероятности реализации угрозы. Список используемых технических представлен в таблице 14.

Таблица 14 – Технические средства

Описание	Идентификатор	Цена	Основные возможности
Межсетевой экран D-Link DFL-260E	ТС1	25300руб.	Осуществляет контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами
Kaspersky Total Security 2015	ТС2	1000 руб.	Антивирусная защита от вредоносных программ Проверка веб-сайтов, файлов и сообщений Высокая скорость работы Анти-Фишинг для защиты ваших личных данных Сетевой экран

Продолжение таблицы 14

Описание	Идентификатор	Цена	Основные возможности
СЗИ от НСД «Secure Tower»	ТС3	Сервер – 20000 руб. Клиент – 5500руб	1 Защита от несанкционированного доступа; 2 Идентификация/аутентификация пользователей для входа в ОС; 3 Статический и динамический контроль целостности данных, их защита от несанкционированных модификаций; 4 Создание индивидуальной для каждого пользователя изолированной программной среды; 5 Запрет запуска неразрешенных программ; 6 Разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа; 7 Разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа; 8 Автоматическое ведение протокола регистрируемых событий; 9 Управление терминальными сессиями; 10 Контроль печати на принтерах, подключенных как к терминальным серверам, так и к пользовательским терминалам. 11 Контроль доступа к USB-устройствам.
Источник бесперебойного питания POWERCOM PTM-650A	ТС4	4000 руб.	1. Мошность 650 ВА; 2. Входное напряжение 140 – 300 В; 3. Частота входного напряжения 50 – 60 Гц; 4. Время переключения батареи 8 мс; 5. Время работы при полной нагрузке 8 минут.
Сетевой помехоподавляющий фильтр ФПБМ – 3	ТС5	15600руб.	Предназначен для защиты от утечки или специально организованной передачи информации по цепям питания 220(380)В/50Гц. Помимо этого, устройство очищает от помех и улучшает форму сетевого напряжения.

Продолжение таблицы 14

Описание	Идентификатор	Цена	Основные возможности
Электронный ключ IButton и устройство считывания IButton RDS-01	ТС6	2800руб.	Обеспечивает вход в систему только пользователям обладающим персональным идентификатором.
Номерные пломбы наклейки СКР1	ТС7	4 руб.	Обеспечивает контроль НСД к оборудованию

Список требований к защитным мерам, а также организационные и технические средства для их реализации представлены в таблице 15.

Таблица 15– Выбор защитных меры

Актив	Уязвимость	Угроза	Требования к ЗМ	Обеспечиваемое свойство ИБ	Варианты реализации требований	
					ТС	ОМ
ИА1	УЯ1	У2	ЗМ11, ЗМ13	Ц, Д	ТС3, ТС1	ОМ16, ОМ18
		У6	ЗМ32, ЗМ33, ЗМ42	К, Ц	ТС1, ТС2, ТС3	ОМ6, ОМ8, ОМ9
		У9	ЗМ27, 28	Ц, Д	ТС1, ТС2	ОМ9, ОМ12, ОМ16
		У11	ЗМ11, ЗМ13	Ц, Д	ТС3, ТС1	-
	УЯ2	У2	ЗМ3, ЗМ11	Д	ТС1, ТС3, ТС4	-
		У4	ЗМ32, ЗМ37	Д	ТС3, ТС5	ОМ19, ОМ20
	УЯ3	У4	-	-	-	-
		У5	ЗМ1, ЗМ2	К, Д	ТС1, ТС3	-
	УЯ4	У3	ЗМ3, ЗМ20	К	ТС3	ОМ3, ОМ13
		У6	ЗМ32, ЗМ45	К, Ц	ТС1, ТС3	ОМ2, ОМ16
		У7	ЗМ46, ЗМ47, ЗМ48	К	ТС3, ТС6	ОМ21, ОМ22

Продолжение таблицы 15

Актив	Уязвимость	Угроза	Требования к ЗМ	Обеспечиваемое свойство ИБ	Варианты реализации требований	
					ТС	ОМ
ИА1	УЯ4	У10	ЗМ42, ЗМ44, ЗМ48	К, Ц	ТС1, ТС3, ТС6	ОМ1, ОМ2, ОМ6
		У11	ЗМ45, ЗМ47	К, Ц	ТС3, ТС6	ОМ1, ОМ7
	УЯ5	У5	ЗМ20, ЗМ27	Д	ТС3	-
	УЯ6	У2	ЗМ20, ЗМ23	Ц	ТС3, ТС7	ОМ8, ОМ14
		У6	ЗМ43, ЗМ45	К, Ц	ТС3	ОМ8, ОМ10
		У9	ЗМ11, ЗМ3	Ц, Д	ТС1, ТС2	ОМ9, ОМ11, ОМ12
		У10	ЗМ9, ЗМ11, ЗМ27	К	ТС3	ОМ2, ОМ3
	УЯ7	У3	ЗМ28, ЗМ34, ЗМ36	Д	ТС1, ТС3	ОМ8, ОМ13
	УЯ9	У1	ЗМ21, ЗМ23	Д	ТС4, ТС5	ОМ13
		У7	ЗМ14, ЗМ42	К, Ц	ТС3	ОМ13, ОМ16, ОМ17
	УЯ10	У1	ЗМ15, ЗМ16	Д	ТС4, ТС5	ОМ13
ИА2	УЯ1	У2	ЗМ11, ЗМ13	Ц, Д	ТС3, ТС1	ОМ16, ОМ18
		У6	ЗМ32, ЗМ33, ЗМ42	К, Ц	ТС1, ТС2, ТС3	ОМ6, ОМ8, ОМ9
		У9	ЗМ27, 28	Ц, Д	ТС1, ТС2	ОМ9, ОМ12, ОМ16
		У11				
	УЯ2	У2	-	-	-	-
		У4	ЗМ32, ЗМ37	Д	ТС3, ТС5	ОМ19, ОМ20
	УЯ3	У4				
	УЯ4	У3	ЗМ3, ЗМ20	К	ТС3	ОМ3, ОМ13
		У6	ЗМ32, ЗМ45	К, Ц	ТС1, ТС3	ОМ2, ОМ16
		У7	ЗМ46, ЗМ47, ЗМ48	К	ТС3, ТС6	ОМ21, ОМ22
		У10	ЗМ42, ЗМ44, ЗМ48	К, Ц	ТС1, ТС3, ТС6	ОМ1, ОМ2, ОМ5
		У11	ЗМ45, ЗМ47	К, Ц	ТС3, ТС6	ОМ1, ОМ7

Продолжение таблицы 15

Актив	Уязвимость	Угроза	Требования к ЗМ	Обеспечиваемое свойство ИБ	Варианты реализации требований	
					ТС	ОМ
ИА2	УЯ6	У2	ЗМ20, ЗМ23	Ц	ТС3, ТС7	ОМ8, ОМ14
		У6	ЗМ43, ЗМ45	К, Ц	ТС3	ОМ8, ОМ10
		У9	ЗМ11, ЗМ3	Ц, Д	ТС1, ТС2	ОМ9, ОМ11, ОМ12
		У10	ЗМ9, ЗМ11, ЗМ27	К	ТС3	ОМ2, ОМ3
ИА2	УЯ7	У3	ЗМ28, ЗМ34, ЗМ36	Д	ТС1, ТС3	ОМ8, ОМ13
	УЯ8	У3	ЗМ39, ЗМ40	К, Д	ТС3, ТС6, ТС7	ОМ1, ОМ4 , ОМ17
	УЯ9	У1	ЗМ21, ЗМ23	Д	ТС4, ТС5	ОМ13
		У7	ЗМ14, ЗМ42	К, Ц	ТС3	ОМ13, ОМ16, ОМ17
	УЯ10	У1	ЗМ15, ЗМ16	Д	ТС4, ТС5	ОМ13
ИА3	УЯ1	У6	ЗМ32, ЗМ33, ЗМ42	К, Ц	ТС1, ТС2, ТС3	ОМ6, ОМ8, ОМ9
		У11				
	УЯ4	У3	ЗМ3, ЗМ20	К	ТС3	ОМ3, ОМ13
		У6	ЗМ32, ЗМ45	К, Ц	ТС1, ТС3	ОМ2, ОМ16
		У7	ЗМ46, ЗМ47, ЗМ48	К	ТС3, ТС6	ОМ21, ОМ22
		У11	ЗМ45, ЗМ47	К, Ц	ТС3, ТС6	ОМ1, ОМ7
	УЯ8	У3	ЗМ39, ЗМ40	К, Д	ТС3, ТС6, ТС7	ОМ1, ОМ4 , ОМ17
	УЯ9	У1	ЗМ21, ЗМ23	Д	ТС4, ТС5	ОМ13
	УЯ10	У1	ЗМ15, ЗМ16	Д	ТС4, ТС5	ОМ13
ИА4	УЯ4	У7	ЗМ46, ЗМ47, ЗМ48	К	ТС3, ТС6	ОМ21, ОМ22
	УЯ7	У7	ЗМ34, ЗМ36	К, Ц	ТС1, ТС3	ОМ10

Продолжение таблицы 15

Актив	Уязвимость	Угроза	Требования к ЗМ	Обеспечиваемое свойство ИБ	Варианты реализации требований	
					ТС	ОМ
ВА1	УЯ2	У2				
	УЯ3	У5	ЗМ1, ЗМ2	К, Д	ТС1, ТС3	-
	УЯ4	У3	ЗМ3, ЗМ20	К	ТС3	ОМ3, ОМ13
	УЯ5	У5	ЗМ20, ЗМ27	Д	ТС3	-
	УЯ6	У2	ЗМ20, ЗМ23	Ц	ТС3, ТС7	ОМ8, ОМ14
	УЯ7	У3	ЗМ28, ЗМ34, ЗМ36	Д	ТС1, ТС3	ОМ8, ОМ13
	УЯ8	У3	ЗМ39, ЗМ40	К, Д	ТС3, ТС6, ТС7	ОМ1, ОМ4 , ОМ17
	УЯ9	У1	ЗМ21, ЗМ23	Д	ТС4, ТС5	ОМ13
ВА2	УЯ1	У9	ЗМ27, 28	Ц, Д	ТС1, ТС2	ОМ9, ОМ12, ОМ16
		У11				
	УЯ2	У2				
		У4	ЗМ32, ЗМ37	Д	ТС3, ТС5	ОМ19, ОМ20
	УЯ3	У4				
	УЯ6	У2	ЗМ20, ЗМ23	Ц	ТС3, ТС7	ОМ8, ОМ14
		У9	ЗМ11, ЗМ3	Ц, Д	ТС1, ТС2	ОМ9, ОМ11, ОМ12
	УЯ9	У1	ЗМ21, ЗМ23	Д	ТС4, ТС5	ОМ13
	УЯ10	У1	ЗМ15, ЗМ16	Д	ТС4, ТС5	ОМ13
ВА3	УЯ1	У6	ЗМ11, ЗМ13	Ц, Д	ТС3, ТС1	ОМ16, ОМ18
		У9	ЗМ32, ЗМ33, ЗМ42	К, Ц	ТС1, ТС2, ТС3	ОМ6, ОМ8, ОМ9
		У11	ЗМ27, 28	Ц, Д	ТС1, ТС2	ОМ9, ОМ12, ОМ16
	УЯ2	У2	-	-	-	-
		У4	ЗМ32, ЗМ37	Д	ТС3, ТС5	ОМ19, ОМ20
	УЯ3	У4				
	УЯ4	У3	ЗМ3, ЗМ20	К	ТС3	ОМ3, ОМ13

Продолжение таблицы 15

Актив	Уязвимость	Угроза	Требования к ЗМ	Обеспечиваемое свойство ИБ	Варианты реализации требований	
					ТС	ОМ
ВА3	УЯ4	У6	ЗМ32, ЗМ45	К, Ц	ТС1, ТС3	ОМ2, ОМ16
		У11	ЗМ45, ЗМ47	К, Ц	ТС3, ТС6	ОМ1, ОМ7
	УЯ6	У2	ЗМ20, ЗМ23	Ц	ТС3, ТС7	ОМ8, ОМ14
		У6	ЗМ43, ЗМ45	К, Ц	ТС3	ОМ8, ОМ10
		У9	ЗМ11, ЗМ3	Ц, Д	ТС1, ТС2	ОМ9, ОМ11, ОМ12
	УЯ7	У3	ЗМ28, ЗМ34, ЗМ36	Д	ТС1, ТС3	ОМ8, ОМ13
	УЯ8	У3	ЗМ39, ЗМ40	К, Д	ТС3, ТС6, ТС7	ОМ1, ОМ4, ОМ17
		У8	ЗМ39, ЗМ40	Д, Ц	ТС2, ТС3	ОМ9, ОМ12
ВА4	УЯ1	У11	ЗМ27, 28	Ц, Д	ТС1, ТС2	ОМ9, ОМ12, ОМ16
	УЯ4	У11	ЗМ45, ЗМ47	К, Ц	ТС3, ТС6	ОМ1, ОМ7
	УЯ8	У8	ЗМ39, ЗМ40	Д, Ц	ТС2, ТС3	ОМ9, ОМ12

В результате выполнения, для всех сценариев ранг угрозы, которых не превышает 4 в соответствии с ГОСТ Р ИСО/МЭК 27002-2012 выбран перечень защитных мер, также для каждого сценария произведен выбор наиболее актуальных технических средств и организационных мер

Наиболее актуальным техническим средством является СЗИ от НСД «Secure Tower» так, как данное ТС осуществляет мониторинг рабочих станций отдела, выполняет контроль целостности и конфиденциальности.

5 Разработка политик информационной безопасности автоматизированной системы для областей обеспечения информационной безопасности

В соответствии с требованиями организации, для подразделений, работающих с программно-аппаратными средствами с предустановленной ОС embox были разработаны частные политики информационной (ИБ) безопасности для следующих областей обеспечения ИБ:

- приобретение, разработка и эксплуатация информационных систем;
- менеджмент непрерывности бизнеса;
- менеджмент коммуникаций и работ.
- контроль доступа

Разработанные политики ИБ представлены в приложении А.

ЗАКЛЮЧЕНИЕ

В процессе выполнения выпускной квалификационной работы выполнено описание функциональных возможностей и особенностей операционной системы embox. Идентифицирована среда использования ОС. Идентифицированы угрозы и уязвимости ИС, в которой применяется аппаратура с ОС embox.

Произведены анализ и оценивание риска, определены способы обработки рисков, и в соответствии с ГОСТ Р ИСО/МЭК 27002-2012 выбраны защитные меры. Также для минимизации вероятности угрозы разработаны организационные меры и выбраны технические средства.

В результате проделанной работы осуществлены оценка и анализ риска, разработан перечень организационных мер, осуществлен выбор наиболее актуальных технических средств, выполнена разработка частных политик информационной безопасности в областях, указанных руководством данного подразделения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Бондарев А.В. ОС Embox: решение для встроенных систем [электронный ресурс] // bit.samag.ru: журнал бизнес и информационные технологии 10 июня 2015, выпуск 5. URL: http://bit.samag.ru/archive/more/152;

2 Терехов А.Н. конфигурируемая ОС РВ Embox для встроенных систем [электронный ресурс] // http://samag.ru: журнал системный администратор 2015, выпуск 7-8. URL: http://samag.ru/archive/article/3001;

3 Особенности ОС РВ FreeRTOS [электронный ресурс] // freertos.org: сайт разработчика. URL: http://shop.freertos.org/FreeRTOS_tutorial_books_and_reference_manuals_s/1825.htm ;

4Особенности ОС РВ eCos [электронный ресурс] // ecos.org: сайт разработчика. URL http://ecos.sourceware.org/fom-serv/ecos/cache/19.html;

5Банк данных угроз безопасности [электронный ресурс] // fstec.ru: банк данных угроз. URL: http://bdu.fstec.ru/threat ;

6ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;

7ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

8ГОСТ 7.0.5 2008 Библиографическая ссылка. Общие требования и правила составления.

ПРИЛОЖЕНИЕ А

Частные политики информационной безопасности

УТВЕРЖДЕНА
решением совета директоров:
Пензенский научно-исследовательский
электротехнический институт

Приказ №

Частная политика информационной безопасности отдела «АО ПНИЭИ» занимающегося разработкой ПО, в сфере «Приобретение, разработка и эксплуатация информационных систем»

Пенза 2016

Введение

Политика информационной безопасности «АО ПНИЭИ» в области «Приобретение, разработка и эксплуатация информационных систем» определяет цели и основные принципы системы обеспечения информационной безопасности (ИБ) подразделения осуществляющего тестирование ПО и использующего в своей деятельности программно-аппаратные средства с предустановленной ОС embox в рассматриваемой сфере и устанавливает основные правила, требования и руководящие принципы в области обеспечения ИБ, которыми руководствуется подразделения и сотрудники в своей повседневной деятельности.

1 Цели обеспечения информационной безопасности

Целью обеспечения ИБ подразделения «АО ПНИЭИ» в сфере «Приобретение, разработка и эксплуатация информационных систем» является обеспечение возможности и непрерывности эксплуатации информационной системы и основных её компонентов для осуществления бизнес-деятельности организации.

2 Область действия политики

Объектами защиты в данной области ИБ являются активы, приведённые в таблицах А.1 и А.2.

Таблица А.1 – Перечень информационных активов и их ценность

Обозначение информационного актива	Описание	Ценность
ИА1	Код исследуемой программы (ИА1)	В
ИА2	Техническое задание (ИА2)	С
ИА3	Информация о подразделении (ИА3)	С
ИА4	Пдн лица выполняющего тестирования (ИА4)	В

Таблица А.2 – Перечень вспомогательных активов и их ценность

Обозначение вспомогательного актива	Описание	Ценность
ВА1	АО	В

Продолжение таблицы А.2

Обозначение вспомогательного актива	Описание	Ценность
ВА2	ПО	С
ВА3	База данных	С
ВА4	Разработчик	В

3 Риски информационной безопасности (ИБ), связанные с объектами защиты

Описание рисков в данной сфере обеспечения информационной безопасности организации приведено ниже:

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путём реализации угрозы «Нарушение энергоснабжения» с использование уязвимости «Отсутствие надлежащего распределения обязанностей по обеспечению ИБ совместно с уязвимостью «Недостаточное техническое обслуживание»;

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путем реализации угрозы «Отказ телекоммуникационного оборудования» с использованием уязвимости «слабость сетевых протоколов, ошибки в ходе реализации протоколов»;

– потеря репутации, вследствие нарушения конфиденциальности информационных активов: «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование», путём реализации угрозы «Преступное использование аппаратных средств» с использованием уязвимости «Ошибки в настройке системы разграничения доступа к объектам файловой системы»;

– финансовые затраты связанные, со стоимостью восстановления резервной копии актива вследствие нарушения целостности информационных активов: «Код исследуемой программы», «Техническое задание», путем реализации угрозы «Доступ к защищаемым файлам с использованием обходного пути» с использованием уязвимости «Отсутствие контроля изменений конфигураций аппаратного и программного обеспечения»;

– потеря репутации, вследствие нарушения конфиденциальности информационных активов: «Код исследуемой программы», «Техническое задание», путем реализации угрозы «Несанкционированный доступ к информации, хранящейся в БД» с использованием уязвимости «Слабость сетевых протоколов, ошибки, допущенные в реализации протоколов».

4 Субъекты и роли, на которые распространяется действие данной политики

Данная политика распространяется на подразделение «АО ПНИЭИ» занимающееся тестированием ПО и использующее в своей работе программно аппаратные средства с предустановленной ОС embox.

Особое значение данная политика имеет для сотрудников подразделения использующих в своей работе программно-аппаратные средства с ОС embox, а также для отдела безопасности курирующего выполнение данной политики.

5 Требования информационной безопасности и правила, которые необходимо выполнять

В данной области ИБ следует руководствовать следующими требованиями:

– в приложениях и иных программных средах должны быть встроены валидационные проверки, с целью предотвратить любую порчу информации вследствие ошибок обработки или умышленных действий;

– возможности для утечки информации должны предупреждаться. Перечень технических средств для реализации требования ИБ

6 Перечень технических средств, реализующих требования ИБ приведён ниже:

– СЗИ от НСД «Secure Tower»;

– Электронный ключ IButton;

– Источник бесперебойного питания POWERCOM PTM-650A.

7 Перечень организационных мер для реализации требований ИБ

Перечень организационных мер, реализующих требования ИБ приведён ниже:

– составление списка лиц, допущенных к системной документации;

– внедрение механизма контроля целостности;

– обновление антивирусных баз;

– наблюдение за деятельностью персонала там, где это разрешено.

8 Обязанности по обеспечению информационной безопасности в рамках данной области, описание функции субъектов над управляемыми объектами

Обязанности совета директоров:

– утверждение политики информационной безопасности(ИБ) в сфере «приобретение, разработка и эксплуатация информационных систем»;

– проведение собеседований при приеме на работу;

– организация курсов по повышению квалификации;

Функции совета директоров:

Участие в идентификации, оценке рисков ИБ в данной области ИБ, утверждение перечня технических средств и организационных мер для минимизации рисков.

Функции отдела безопасности:

– контроль реализации данной политики;

– участие в обработке инцидентов в данной сфере ИБ;

– осуществлять контроль деятельности персонала на рабочих местах;

– проведение внеплановых проверок знаний работников.

9 Состав ссылочных документов

Для адекватного понимания текста данной политики необходимо ознакомиться со следующими документами:

– «Корпоративная политика информационной безопасности «АО ПНИЭИ», утверждённая приказом №23 советом директоров - председатель ФИО от 28.02.2015;

– ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10 Положения по контролю реализации политики

Выполнение требований ИБ в области приобретения, разработки и эксплуатации информационных систем контролирует отдел безопасности «АО ПНИЭИ».

11 Ответственность за реализацию и поддержку политики

Реализацию и поддержку данной политики осуществляет отдел безопасности в соответствии с обязанностями и функциями, изложенными в п.8 настоящей политики.

12 Условия пересмотра политики

Пересмотр настоящей политики ИБ осуществляется составом должностных лиц, участвующих в её первичном формировании, в следующих случаях:

– в случае выявления аудитом ИБ несоответствия защитных мер, определённых данной политикой ИБ, фактам зафиксированных инцидентов ИБ, или отсутствие таких защитных мер;

– при существенных изменениях в бизнес-процессах организации;

– при изменениях законодательства РФ в части ИБ.

Председатель совета директоров

_____

подпись

УТВЕРЖДЕНА
решением совета директоров:
Пензенский научно-исследовательский
электротехнический институт

Приказ №

Частная политика информационной безопасности отдела «АО ПНИЭИ» занимающегося разработкой ПО, в сфере «Менеджмент непрерывности бизнеса»

Пенза 2016

Введение

Политика информационной безопасности подразделения «АО ПНИЭИ» в области «Менеджмент непрерывности бизнеса» определяет цели и основные принципы системы обеспечения информационной безопасности (ИБ) в рассматриваемой сфере и устанавливает основные правила, требования и руководящие принципы в области обеспечения ИБ, которыми руководствуется подразделение и его сотрудники в своей повседневной деятельности.

1 Цели обеспечения информационной безопасности

Целью обеспечения ИБ подразделения «АО ПНИЭИ» в сфере «Менеджмент непрерывности бизнеса» является обеспечение непрерывности выполнения бизнес-процессов организации.

2 Область действия политики

Объектами защиты в данной области ИБ являются активы, приведённые в таблицах А.3 и А.4.

Таблица А.3 – Перечень информационных активов и их ценность

Обозначение информационного актива	Описание	Ценность
ИА1	Код исследуемой программы (ИА1)	В
ИА2	Техническое задание (ИА2)	С
ИА3	Информация о подразделении (ИА3)	С
ИА4	Пдн лица выполняющего тестирования (ИА4)	В

Таблица А.4 – Перечень вспомогательных активов и их ценность

Обозначение вспомогательного актива	Описание	Ценность
ВА1	АО	В
ВА2	ПО	С

Продолжение таблицы А.4

Обозначение вспомогательного актива	Описание	Ценность
ВА3	База данных	С
ВА4	Разработчик	В

3 Риски информационной безопасности (ИБ), связанные с объектами защиты

Описание рисков в данной сфере обеспечения информационной безопасности организации приведено ниже:

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путём реализации угрозы «Нарушение энергоснабжения» с использование уязвимости «Отсутствие надлежащего распределения обязанностей по обеспечению ИБ», совместно с уязвимостью «Недостаточное техническое обслуживание»;

– потери времени, частичное или полное прерывание деятельности организации, потери репутации вследствие нарушения законодательных требований вследствие нарушения доступности информационных активов «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путем реализации угрозы «Отказ телекоммуникационного оборудования» с использованием уязвимости «Слабость сетевых протоколов, ошибки в ходе реализации протоколов» совместно с уязвимостью «Уязвимость, внедряемая автоматизированными средствами проектирования/разработки»;

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание» путем реализации угрозы «Нарушение функционирования программного обеспечения» с использованием уязвимости «Недостаточность мер по контролю за ошибками

в ходе проектирования систем, связанных с безопасностью» совместно с уязвимостью «Уязвимость, внедряемая автоматизированными средствами проектирования/разработки»;

– потери времени, частичное или полное прерывание деятельности, финансовые затраты связанные со стоимостью восстановления резервной копии актива организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путем реализации угрозы «Угроза доступа к защищаемым файлам с использованием обходного пути» с использованием уязвимостей «Ошибки в настройке системы разграничения доступа к объектам файловой системы» и «Отсутствие контроля изменений конфигураций аппаратного и программного обеспечения»;

4 Субъекты и роли, на которые распространяется действие данной политики

Данная политика распространяется на подразделение «АО ПНИЭИ» занимающееся тестированием ПО и использующее в своей работе программно аппаратные средства с предустановленной ОС embox.

Особое значение данная политика имеет для сотрудников подразделения использующих в своей работе программно-аппаратные средства с ОС embox,

5 Требования информационной безопасности и правила, которые необходимо выполнять

В данной области ИБ следует руководствоваться следующим основным требованием – следует разработать и внедрить планы обеспечения непрерывности бизнеса с целью поддержки или восстановления операций и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или сбоя критических процессов бизнеса.

6 Перечень технических средств для реализации требования ИБ

– источник бесперебойного питания POWERCOM PTM-650A;

– сетевой помехоподавляющий фильтр ФПБМ. – 3.

7 Перечень организационных мер для реализации требований ИБ

В данной области обеспечения ИБ применяются следующие организационные меры:

– разработка и внедрение планов непрерывности бизнеса;

– разработка процедуры хранения системной документации и съёмных носителей информации.

– резервное копирование информации и конфигураций с сервера БД необходимо проводить 2 раза в месяц.

8 Обязанности по обеспечению информационной безопасности в рамках данной области, описание функции субъектов над управляемыми объектами

Обязанности совета директоров:

– утверждение политики информационной безопасности(ИБ) в сфере «Менеджмент непрерывности бизнеса»;

– проведение собеседований при приеме на работу;

– утверждение плана обеспечения непрерывности бизнеса;

Функции совета директоров:

Участие в идентификации, оценке рисков ИБ в данной области ИБ, утверждение перечня технических средств и организационных мер для минимизации рисков.

Функции отдела безопасности:

– контроль реализации данной политики;

– участие в обработке инцидентов в данной сфере ИБ;

– участие в разработке плана обеспечения непрерывности бизнеса;

9 Состав ссылочных документов

Для адекватного понимания текста данной политики необходимо ознакомиться со следующими документами:

– «Корпоративная политика информационной безопасности «АО ПНИЭИ», утверждённая приказом №23 советом директоров - председатель ФИО от 28.02.2015;

– ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10 Положения по контролю реализации политики

Выполнение требований в области ИБ менеджмент непрерывности бизнеса контролирует отдел безопасности «АО ПНИЭИ».

Для проверки реализации ИБ подразделения в данной сфере проводится внутренний аудит системы.

11 Ответственность за реализацию и поддержку политики

Реализацию и поддержку данной политики осуществляет отдел безопасности в соответствии с обязанностями и функциями, изложенными в п.8 настоящей политики.

12 Условия пересмотра политики

Пересмотр настоящей политики ИБ осуществляется составом должностных лиц, участвующих в её первичном формировании, в следующих случаях:

– в случае выявления аудитом ИБ несоответствия защитных мер, определённых данной политикой ИБ, фактам зафиксированных инцидентов ИБ, или отсутствие таких защитных мер;

– при существенных изменениях в бизнес-процессах организации;

– при изменениях законодательства РФ в части ИБ.

Председатель совета директоров

_____

подпись

УТВЕРЖДЕНА
решением совета директоров:
Пензенский научно-исследовательский
электротехнический институт

Приказ №

Частная политика информационной безопасности отдела «АО ПНИЭИ» занимающегося разработкой ПО, в сфере «Менеджмент коммуникаций и работ»

Пенза 2016

Введение

Политика информационной безопасности подразделения «АО ПНИЭИ» в области «Менеджмент коммуникаций и работ» определяет цели и основные принципы системы обеспечения информационной безопасности (ИБ) подразделения в рассматриваемой сфере и устанавливает основные правила, требования и руководящие принципы в области обеспечения ИБ, которыми руководствуется отдел и его сотрудники в своей повседневной деятельности.

1 Цели обеспечения информационной безопасности

Целью обеспечения ИБ подразделения «АО ПНИЭИ» в сфере «Менеджмент коммуникаций и работ» является обеспечение функционирования процессов сбора, обработки, хранения и передачи информации.

2 Область действия политики

Объектами защиты в данной области ИБ являются активы, приведённые в таблицах А.5 и А.6.

Таблица А.5 – Перечень информационных активов и их ценность

Обозначение информационного актива	Описание	Ценность
ИА1	Код исследуемой программы (ИА1)	B
ИА2	Техническое задание (ИА2)	C
ИА3	Информация о подразделении (ИА3)	C
ИА4	Пдн лица выполняющего тестирования (ИА4)	B

Таблица А.6 – Перечень вспомогательных активов и их ценность

Обозначение вспомогательного актива	Описание	Ценность
ВА1	АО	B
ВА2	ПО	C

Продолжение таблицы А.4

Обозначение вспомогательного актива	Описание	Ценность
ВА3	База данных	С
ВА4	Разработчик	В

3 Риски информационной безопасности (ИБ), связанные с объектами защиты

Описание рисков в данной сфере обеспечения информационной безопасности организации приведено ниже:

– потери репутации вследствие нарушения законодательных требований, финансовые затраты связанные со стоимостью восстановления резервной копии актива организации вследствие нарушения целостности информационных активов: «Код исследуемой программы», «Техническое задание», «Информация о подразделении» путем реализации угрозы «Преступное использование аппаратных средств» с использованием уязвимостей «Отсутствие политик использования телекоммуникационной среды обмена сообщениями» и «Отсутствие регулярных аудитов;

– потери время на восстановление, потеря репутации в следствии нарушения законодательных требований в следствии нарушения доступности актива «Код исследуемой программы» путем реализации угрозы «Включение в проект не достоверно испытанных компонентов» с использованием уязвимости «Недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью», совместно с «Возможностью выхода из строя критически важного модуля»;

– финансовые затраты связанные со стоимостью восстановления резервной копии актива организации вследствие нарушения целостности информационного актива: «Информация о подразделении» путем реализации угрозы «Искажение информации, хранящейся в БД» с использованием уязвимости «Отсутствие регулярных аудитов»;

– потери репутации вследствие нарушения законодательных требований, финансовые затраты связанные со стоимостью восстановления резервной копии актива организации вследствие нарушения целостности информационных активов: «Код исследуемой программы», «Техническое задание», «Информация о подразделении» путем реализации угрозы «Несанкционированный доступ к информации хранящейся в БД» с использованием уязвимости «Слабость сетевых протоколов, ошибки допущенные в ходе реализации протоколов» совместно с «Ошибки в системе разграничения доступа к объектам файловой системы».

4 Субъекты и роли, на которые распространяется действие данной политики

Данная политика распространяется на подразделение «АО ПНИЭИ» занимающееся тестированием ПО и использующее в своей работе программно аппаратные средства с предустановленной ОС embox.

Особое значение данная политика имеет для сотрудников подразделения использующих в своей работе программно-аппаратные средства с ОС embox,

5 Требования информационной безопасности и правила, которые необходимо выполнять

В данной области ИБ следует руководствоваться следующими основными требованиями:

– обязанности и области ответственности должны быть разделены для уменьшения возможностей неавторизованной или непреднамеренной модификации активов организации или их нецелевого использования;

– необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей;

– резервное копирование информации и программного обеспечения должно выполняться и тестироваться на регулярной основе в соответствии с установленной политикой резервирования;

– сети должны адекватно управляться и контролироваться, чтобы быть защищенными от угроз и обеспечить безопасность систем и прикладных программ, использующих сеть, включая информацию во время ее передачи;

– должны существовать процедуры в отношении менеджмента сменных носителей информации;

– с целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации;

– системная документация должна быть защищена от неавторизованного доступа;

– необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом.

6 Перечень технических средств для реализации требования ИБ

Для обеспечения БИ в данной сфере используются следующие ТС:

– СЗИ от НСД «Secure Tower»;

– межсетевой экран D-Link DFL-260E

– антивирус «Kaspersky Total Security 2015»

7 Перечень организационных мер для реализации требований ИБ

В данной области ИБ применяются следующие основные организационные меры:

– для каждого носителя информации (бумажного или электронного) составление списка лиц, допущенных к нему;

– ограничение доступа к информации, хранящейся на компьютерах;

– составление списка лиц, допущенных к системной документации;

– разработка процедуры хранения системной документации и съёмных носителей информации;

– должен быть разработан журнал учёта съёмных носителей информации;

– должен быть разработан перечень обязанностей для каждого должностного лица;

– резервное копирование информации и конфигураций с сервера БД необходимо проводить 2 раза в месяц;

– носители с резервными копиями подвергаются шифрованию;

– осуществлять проверку обновления антивирусных бах 1 раз в 3 дней;

– осуществлять сканирование компьютеров на наличие вирусов 1 раз в 3 дней;

– необходимо вести аудит всех действий пользователей и администраторов;

– хранение журналов регистрации события осуществлять в течение 2-х месяцев;

– назначение ответственного за сеть организации;

– разработка и ведение журнала учёта неисправностей.

8 Обязанности по обеспечению информационной безопасности в рамках данной области, описание функции субъектов над управляемыми объектами

Обязанности совета директоров:

– утверждение политики информационной безопасности(ИБ) в сфере «Менеджмент коммуникационных работ»;

– участие в разработке и утверждение списка разграничения доступа к съёмным носителям информации;

– участие в разработке и утверждение списка лиц, допущенных к системной документации;

– участие в разработке и утверждение списка должностных обязанностей для каждого должностного лица;

– утверждение журнала учёта съёмных носителей информации;

– утверждение журнала учёта неисправностей;

– утверждение процедуры хранения системной документации и съёмных носителей информации;

Функции совета директоров:

Участие в идентификации, оценке рисков ИБ в данной области ИБ, утверждение перечня технических средств и организационных мер для минимизации рисков.

Функции отдела безопасности:

– контроль реализации политики;

– участие в обработке инцидентов;

– ведение журнала учёта неисправностей;

– участие в разработке списка должностных обязанностей для каждого должностного лица;

– участие в разработке списка разграничения доступа к съёмным носителям информации;

– участие в разработке и утверждение списка лиц, допущенных к системной документации;

– участие в разработке процедуры хранения системной документации и съёмных носителей информации;

– выдача съёмных носителей информации под роспись в журнале их учёта.

9 Состав ссылочных документов

Для адекватного понимания текста данной политики необходимо ознакомиться со следующими документами:

– «Корпоративная политика информационной безопасности «АО ПНИЭИ», утверждённая приказом №23 советом директоров - председатель ФИО от 28.02.2015;

– ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10 Положения по контролю реализации политики

Выполнение требований в области ИБ менеджмент непрерывности бизнеса контролирует отдел безопасности «АО ПНИЭИ».

Для проверки реализации ИБ подразделения в данной сфере проводится внутренний аудит системы.

11 Ответственность за реализацию и поддержку политики

Реализацию и поддержку данной политики осуществляет отдел безопасности в соответствии с обязанностями и функциями, изложенными в п.8 настоящей политики.

12 Условия пересмотра политики

Пересмотр настоящей политики ИБ осуществляется составом должностных лиц, участвующих в её первичном формировании, в следующих случаях:

– в случае выявления аудитом ИБ несоответствия защитных мер, определённых данной политикой ИБ, фактам зафиксированных инцидентов ИБ, или отсутствие таких защитных мер;

– при существенных изменениях в бизнес-процессах организации;

– при изменениях законодательства РФ в части ИБ.

Председатель совета директоров

_____

подпись

УТВЕРЖДЕНА
решением совета директоров:
Пензенский научно-исследовательский
электротехнический институт

Приказ №

Частная политика информационной безопасности отдела «АО ПНИЭИ» занимающегося разработкой ПО, в сфере «Контроль доступа»

Пенза 2016

Введение

Политика информационной безопасности АО ПНИЭИ» в области «Контроль доступа» определяет цели и основные принципы системы обеспечения информационной безопасности (ИБ) подразделения в рассматриваемой сфере и устанавливает основные правила, требования и руководящие принципы в области обеспечения ИБ.

1 Цели обеспечения информационной безопасности

Целью обеспечения ИБ подразделения «АО ПНИЭИ» в сфере «Контроль доступа» является обеспечение контроля доступа к информации, хранящейся в БД, а также на локальных машинах. Контроля доступа к аппаратным средствам, программному обеспечению. Обеспечение непрерывности эксплуатации информационной системы и основных её компонентов для осуществления бизнес-деятельности организации.

2 Область действия политики

Объектами защиты в данной области ИБ являются активы, приведённые в таблицах А.7 и А.8.

Таблица А.7 – Перечень информационных активов и их ценность

Обозначение информационного актива	Описание	Ценность
ИА1	Код исследуемой программы (ИА1)	В
ИА2	Техническое задание (ИА2)	С
ИА3	Информация о подразделении (ИА3)	С
ИА4	Пдн лица выполняющего тестирования (ИА4)	В

Таблица А.8 – Перечень вспомогательных активов и их ценность

Обозначение вспомогательного актива	Описание	Ценность
ВА1	АО	В
ВА2	ПО	С

Продолжение таблицы А.4

Обозначение вспомогательного актива	Описание	Ценность
ВА3	База данных	С
ВА4	Разработчик	В

3 Риски информационной безопасности (ИБ), связанные с объектами защиты

Описание рисков в данной сфере обеспечения информационной безопасности организации приведено ниже:

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путём реализации угрозы «Нарушение энергоснабжения» с использование уязвимости «Отсутствие надлежащего распределения обязанностей по обеспечению ИБ», совместно с уязвимостью «Недостаточное техническое обслуживание»;

– потери времени, частичное или полное прерывание деятельности организации, потери репутации вследствие нарушения законодательных требований вследствие нарушения доступности информационных активов «Код исследуемой программы», «Техническое задание», «ПДн лица выполняющего тестирование» путем реализации угрозы «Отказ телекоммуникационного оборудования» с использованием уязвимости «Слабость сетевых протоколов, ошибки в ходе реализации протоколов» совместно с уязвимостью «Уязвимость, внедряемая автоматизированными средствами проектирования/разработки»;

– потери времени, частичное или полное прерывание деятельности организации вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание» путем реализации угрозы «Нарушение функционирования программного обеспечения» с

использованием уязвимости «Недостаточность мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью» совместно с уязвимостью «Уязвимость, внедряемая автоматизированными средствами проектирования/разработки»;

– потери времени, частичное или полное прерывание деятельности организации, финансовые затраты связанные, со стоимостью восстановления резервной копии актива вследствие нарушения доступности информационных активов: «Код исследуемой программы», «Техническое задание», путем реализации угрозы «Доступ к защищаемым файлам с использованием обходного пути» с использованием уязвимости «Отсутствие контроля изменений конфигураций аппаратного и программного обеспечения»;

– потери времени, частичное или полное прерывание деятельности организации, потери репутации вследствие нарушения законодательных требований вследствие нарушения целостности активов Код исследуемой программы», «Техническое задание», путем реализации угрозы «Внедрение вредоносного ПО» с использованием уязвимости «Отсутствие контроля изменений конфигураций аппаратного и программного обеспечения» совместно с «Слабость сетевых протоколов, ошибки в ходе реализации протоколов».

4 Субъекты и роли, на которые распространяется действие данной политики

Данная политика распространяется на подразделение «АО ПНИЭИ» занимающееся тестированием ПО и использующее в своей работе программно аппаратные средства с предустановленной ОС embox.

Особое значение данная политика имеет для сотрудников подразделения использующих в своей работе программно-аппаратные средства с ОС embox,

5 Требования информационной безопасности и правила, которые необходимо выполнять

В данной области ИБ следует руководствовать следующими требованиями:

– необходимо внедрить обработку инцидентов информационной безопасности включая сбои системы и потерю обслуживания;

– необходимо, чтобы в политике безопасности организации были учтены требования в отношении безопасности конкретных прикладных программ;

– необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей;

– права доступа к информации должны пересматриваться каждые шесть месяцев, после повышения/понижения сотрудников в должности.

6 Перечень технических средств для реализации требования ИБ

Перечень технических средств, реализующих требования ИБ приведён ниже:

– СЗИ от НСД Secure Tower;

– межсетевой экран D-Link DFL-260E;

– антивирус «Kaspersky Total Security 2015»;

– электронный ключ IButton;

7 Перечень организационных мер для реализации требований ИБ

Перечень организационных мер, реализующих требования ИБ приведён ниже:

– ограничение доступа к информации, хранящейся на компьютерах;

– внедрение механизма контроля целостности;

– резервное копирование информации и конфигураций с сервера БД необходимо проводить 2 раза в месяц;

– необходимо вести аудит всех действий пользователей и администраторов;

– хранение журналов регистрации события осуществлять в течение 6 месяцев;

– хранение журналов выдачи электронных ключей.

8 Обязанности по обеспечению информационной безопасности в рамках данной области, описание функции субъектов над управляемыми объектами

Обязанности совета директоров:

– утверждение политики информационной безопасности(ИБ) в сфере Контроль доступа»;

– заключение договоров с организациями на предмет спец исследований (обнаружение программных и аппаратных закладок);

– прием на работу сотрудников с образованием в области ИБ;

– составление графика аудитов системы.

Функции совета директоров:

Участие в идентификации, оценке рисков ИБ в данной области ИБ, утверждение перечня технических средств и организационных мер для минимизации рисков.

Функции отдела безопасности:

– контроль реализации данной политики;

– участие в обработке инцидентов в данной сфере ИБ;

– осуществление аудита всех действий пользователей и администраторов.

9 Состав ссылочных документов

Для адекватного понимания текста данной политики необходимо ознакомиться со следующими документами:

– «Корпоративная политика информационной безопасности «АО ПНИЭИ», утверждённая приказом №23 советом директоров - председатель ФИО от 28.02.2015;

– ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10 Положения по контролю реализации политики

Выполнение требований в области ИБ контроль доступа осуществляет отдел безопасности «АО ПНИЭИ».

Для проверки реализации ИБ подразделения в данной сфере проводится внутренний аудит системы.

11 Ответственность за реализацию и поддержку политики

Реализацию и поддержку данной политики осуществляет отдел безопасности в соответствии с обязанностями и функциями, изложенными в п.8 настоящей политики.

12 Условия пересмотра политики

Пересмотр настоящей политики ИБ осуществляется составом должностных лиц, участвующих в её первичном формировании, в следующих случаях:

– в случае выявления аудитом ИБ несоответствия защитных мер, определённых данной политикой ИБ, фактам зафиксированных инцидентов ИБ, или отсутствие таких защитных мер;

– при существенных изменениях в бизнес-процессах организации;

– при изменениях законодательства РФ в части ИБ.

Председатель совета директоров

_____

подпись

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения, информационных технологий и электроники
Выпускающая кафедра:
Информационная безопасность систем и технологий
Учебная группа 11ПИ1

УТВЕРЖДАЮ
Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефиров
27.04 2016 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

студента группы 11ПИ1 Мельникова Антона Витальевича

Специальность 100503 – Информационная безопасность автоматизированных систем

Тема дипломной работы: Оценка рисков информационной безопасности и формирование политики информационной безопасности для операционной системы embox.

Руководитель ВКР
Инженер АО ПНИЭИ Жиркин Александр Алексеевич.

Нормоконтролер
к.т.н., доцент Иванов А.П.

1 Цели и задачи ВКР

Цели работы:

– оценка рисков, возникающих при использовании операционной системы (ОС) embox, и разработка политик безопасности для организаций, использующих аппаратуру с ОС embox.

2 Тактико-технические требования к выполнению ВКР

Технические требования:

– оценка рисков должна содержать:

– идентификацию среды использования операционной системы;

– идентификацию информационных активов;

– идентификацию угроз информационной безопасности;

– идентификация уязвимостей активов информационной системы;

– идентификация существующих защитных мер;

– идентификация последствий.

– анализ риска;

– выбор мер и средств защиты для ОС embox:

– анализ наиболее актуальных программных и технических средств защиты;

– определение способов обработки рисков;

– разработка плана применения программных и технических средств защиты;

– разработка организационных мер по обеспечению ИБ ОС;

– разработка политики безопасности организации применяющих аппаратуру с ОС embox.

В ВКР должны быть рассмотрены следующие вопросы:

– обзор ОС embox;

– сравнительный анализ ОС embox с системами аналогичного класса;

– идентификацию среды использования операционной системы;

– идентификацию информационных активов;

– идентификацию угроз информационной безопасности;

– идентификация уязвимостей активов информационной системы;

– идентификация существующих защитных мер;

– идентификация последствий;

– разработка модели угроз ИБ ОС embox;

– анализ наиболее актуальных программных и технических средств защиты;

– разработка плана применения программных и технических средств защиты;

– разработка организационных мер по обеспечению ИБ ОС;

– разработка политик инормационной безопасности организации применяющих аппаратуру с ОС embox.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

– вертикальное разделение модулей ОС embox - 1л., ф. А1 (плакат);

– сравнительный анализ операционных систем – 1л.,ф.А1 (плакат);

– перечень уязвимостей – 1л., ф. А1 (плакат);

– перечень угроз информационной безопасности - 1л., ф. А1 (плакат);

– перечень программных и технических средств защиты - 1л., ф. А1 (плакат);

– перечень организационных мер обеспечения ИБ - 1л., ф. А1 (плакат);

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ №91 по от 25.04.2016

Дата выдачи задания «11» февраля 2016 г.

Время дипломного проектирования с 11.04 2016 г. по 10.06 2016 г.

Задание к исполнению принял «11» февраля 2016 г.

Исполнитель ВКР _____ Мельников А.В.

Ректору Пензенского
государственного университета
А. Д. Гуляеву
студента 5 курса ФПИТЭ
очной формы обучения
Мельникова Антона Витальевича

заявление.

Я, Мельников Антон Витальевич, студент 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломной работы на тему «Оценка рисков информационной безопасности и формирование политики информационной безопасности для операционной системы openbox», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

/А.В. Мельников /
31.05.2016

ВКР представлена на проверку 31.05.2016

Руководитель ВКР /А.А. Жарких /

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Оценка рисков информационной безопасности и формирование политики информационной безопасности для операционной системы emboxx» студента 5 курса А.В. Мельникова специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР инженер АО «ПНИЭИ» Жиркин Александр Алексеевич.

Отчет о проверке № 1

[redacted]

Информация о документе

[redacted]

Информация об отчете

[redacted]

Оригинальность: 88.67%
Заимствования: 11.33%
Цитирование: 0%

08.06.2016г. А.А. Жиркин

Секретарь ГЭК А.П.Иванов

ОТЗЫВ

на выпускную квалификационную работу студента

Пензенского государственного университета

Мельникова Антона Витальевича

Тема проекта: Оценка рисков информационной безопасности и формирование политики информационной безопасности для операционной системы embox.

Целью квалификационной работы Мельникова Антона Витальевича является оценка рисков, возникающих при использовании операционной системы (ОС) embox, и разработка политик информационной безопасности для организаций, использующих аппаратуру с ОС embox.

Во время выполнения автором был изучен большой объем теоретического и практического материала по описанию операционных систем реального времени, технических особенностях данных операционных систем, были изучены нормативные документы, связанные с оценкой и анализом рисков информационной безопасности. Было выполнено описание функциональных возможностей, а также особенностей операционной системы российских разработчиков embox. В качестве среды использования выбрана плата программно-аппаратного комплекса, с предустановленной на ней ОС embox. Идентификация среды использования позволила определить информационные активы, угрозы и уязвимости для информационной системы, в которой используется данный программно-аппаратный комплекс. На основе идентифицированных угроз и уязвимостей были разработаны сценарии возможных инцидентов, с вероятностями их реализации. Анализ и обработка рисков произведены при помощи нормативных документов ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», и ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». Итогами

проделанной работы являются перечень сценариев инцидентов со способами минимизации их вероятности, а также частные политики информационный безопасности для подразделений организации использующих аппаратуру с предустановленной embox. Разработанные политики подробно описывают перечень необходимых мер и обязанностей персонала в областях, представляющих интерес для руководства подразделения занимающегося исследованием ОС embox.

Следует признать, что такая работа требует большой работоспособности, терпения и упорства, которые Мельников А.В. проявил в полной мере. Ранее дипломник зарекомендовал как ответственный специалист, соблюдающий все сроки и требования, предъявленные к данной ему работе.

Работы по всем пунктам технического задания выполнены полностью. Пояснительная записка и плакаты содержат необходимые сведения о проделанной работе.

Считаю, что дипломный проект выполнен в полном соответствии с заданием и заслуживает оценки «5», а дипломник Мельников Антон Витальевич достоин присвоения квалификации специалиста по информационной безопасности по специальности 10.05.03 – «информационная безопасности автоматизированных систем».

Руководитель ВКР,
инженер АО «ПНИЭИ» /А.А. Жиркин/

10.06.16

ОТДЕЛ КАДРОВ

16 Бланков

РЕЦЕНЗИЯ

На выпускную квалификационную работу студента 5 курса «Пензенского государственного университета» Мельникова Антона Витальевича, обучающегося по специальности «Информационная безопасности» на тему «Оценка рисков информационной безопасности и формирование политики информационной безопасности для операционной системы embox».

Тема выпускной квалификационной работы Мельникова Антона Витальевича посвящена проблеме, оценки рисков информационной безопасности (ИБ) при использовании аппаратуры с предустановленной операционной системой (ОС) реального времени embox. В настоящее время вся аппаратура обработки, передачи информации строится с использованием микроконтроллеров, микропроцессоров, для обеспечения контроля функционирования которых используются операционные системы реального времени. Актуальность данной работы заключается в том, что embox новый продукт на данном рынке, и в настоящее время ведется ее активное исследование, также стоит отметить, что данная ОС является отечественной разработкой.

В работе рассмотрены функциональные возможности операционной системы, представлены особенности архитектуры, а также рассмотрены аспекты информационной безопасности для организации, использующей аппаратуру с предустановленной ОС embox. Автор при написании работы использовал техническую документацию на операционную систему, национальные стандарты в области идентификации и оценки рисков (ГОСТ ИСО/МЭК 27002, ГОСТ ИСО/МЭК 27005, и.д.р.), а также информацию с официальных сайтов разработчиков. Выпускная квалификационная работа написана научным языком, содержит сноски на использованные при ее написании источники, являясь доступной по изложению.

во втором разделе можно было привести анализ более чем двух ОС.

Однако отмеченные недостатки не могут повлиять на общее положительное впечатление от работы, которая соответствует всем предъявляемым требованиям.

Выпускная квалификационная работа Мельникова Антона Витальевича представляет собой самостоятельное исследование и заслуживает оценки « ». «отлично».

Рецензент
зам. начальника отделения АО «ПНИЭИ»
Сомкин Сергей Александрович

Одиннадцать баллов.