Министерство образования и науки РФ
Государственное образовательное учреждение высшего профессионального образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кафедра «Информационная безопасность систем и технологий»

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

Пояснительная записка к курсовому проекту
по дисциплине «ОПОИБ»

ПГУ 3.090106.001 ПЗ

Руководитель КР,
доцент _____Алексеев В. М.
Исполнитель КР,
студент _____Захаров М. А.

Пенза 2010

РЕФЕРАТ

Отчёт 50 с., 2 рис., 12 табл., 4 источников, 2 прил.

ИНФОРМАЦИОННАЯ СИСТЕМА, УЯЗВИМОСТЬ, АКТУАЛЬНАЯ УГРОЗА, ОЦЕНКА РИСКА, ПОЛИТИКА БЕЗОПАСНОСТИ

Объектом исследования является информационная система отделения фонда социального страхования.

Цель работы — получение навыков анализа угроз и разработки политики безопасности информационной системы организации на примере отделения фонда социального страхования.

В процессе работы были идентифицированы объекты защиты в информационной системе, актуальные угрозы для информационных ресурсов отделения фонда социального страхования, разработана политики информационной безопасности информационной системы отделения фонда социального страхования.

В результате исследования была разработана политика информационной безопасности информационной системы отделения фонда социального страхования.

Содержание

Обозначения и сокращения **6**

Введение **7**

1 Идентификация объектов защиты в информационной системе фонда социального страхования **8**

1.1 Цели и задачи фонда 8

1.2 Идентификация информационных процессов 9

1.3 Структура ИС фонда 12

1.4 Идентификация аппаратных ресурсов фонда как объектов защиты 13

1.5 Идентификация информационных ресурсов фонда как объектов защиты 14

1.6 Схема информационных потоков в ИС фонда 15

2 Идентификация актуальных угроз для информационных ресурсов отделения фонда социального страхования **17**

2.1 Описание угроз защищаемым информационным ресурсам 17

2.2 Оценка рисков реализации угроз информационным ресурсам отделения фонда соцального страхования 25

2.3 Определение перечня актуальных угроз информационным ресурсам отделения фонда социального страхования 31

3 Разработка политики ИБ ИС отделения фонда социального страхования **32**

3.1 Формулирование правил противодействия актуальным угрозам информационным ресурсам 32

3.2 Формулирование политики ИБ ИС отделения фонда социального страхования 34

Заключение **36**

Список использованных источников **37**

Приложение А Идентификация аппаратных и информационных ресурсов фонда как объектов защиты **38**

Приложение Б Оценка рисков реализации угроз информационным ресурсам отделения фонда социального страхования **43**

«Утверждаю»
Зав. кафедрой ИБСТ
_____С. Л. Зефиров
«____» _____ 2010 г.

ЗАДАНИЕ
на курсовую работу

по теме: **«Разработка политики информационной безопасности информационной системы организации»**

1 Дисциплина Организационно-правовое обеспечение информационной безопасности

2 Вариант задания Организация — отделение фонда социального страхования. Исходный перечень угроз: нарушение конфиденциальности защищаемой информации, нарушение целостности защищаемой информации. Уровни инфраструктуры: сетевых приложений, операционных систем

3 Студент Захаров М. А. **группа** 06УИ1

4 Исходные данные на проектирование

Должны быть разработаны описание бизнес-функций отделения фонда социального страхования, структура и схема информационных потоков её информационной системы с определенными топологией, количеством рабочих станций, объектами защиты.

Должны быть разработаны описание угроз безопасности информационной системы и сценарии их реализации. Описания угроз и источников угроз должны соответствовать модели ГОСТ Р ИСО/МЭК 15408.

Должны быть оценены риски реализации угроз для полного перечня угроз и определены актуальные для информационной системы угрозы.

Должны быть сформулированы правила информационной безопасности для противодействия угрозам информационной системы отделения фонда социального страхования.

Должна быть разработана политика информационной безопасности информационной системы отделения фонда социального страхования на основе сформулированных правил.

5 Структура проекта

5.1 Пояснительная записка (содержание работы):

– описание информационных процессов организации, идентификация объектов защиты;

– структура информационной системы отделения фонда социального страхования и схема информационных потоков;
– анализ угроз информационным ресурсам;
– оценка рисков реализации угроз, выявление актуальных угроз;
– разработка политики информационной безопасности информационной системы отделения фонда социального страхования.

5.2 Графическая часть

– структура информационной системы отделения фонда социального страхования;
– схема информационных потоков в информационной системе отделения фонда социального страхования.

6 Календарный план выполнения проекта

6.1 Сроки выполнения работ по разделам:

– утверждение ТЗ к 22.02.2010 г.
– идентификация объектов защиты к 08.03.2010 г.
– идентификация актуальных угроз к 12.04.2010 г.
– разработка политики ИБ к 19.04.2010 г.
– оформление и проверка отчёта о КР к 10.05.2010 г.
– подготовка к защите курсовой работы к 24.05.2010 г.

Дата защиты проекта 2010 г.
Руководитель работы Алексеев В. М.
Задание получил 8 февраля 2010 г.
Студент Захаров М. А.
Нормоконтролёр Алексеев В. М.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ — атоматизированное рабочее место
БД — база данных
ИБ — информационная безопасность
ИС — информационная система
ОС — операционная система
ПО — программное обеспечение
СУБД — система управления базами данных
НСД — несанкционированный доступ

ВВЕДЕНИЕ

Информация — это имущество (или активы), которое, подобно другим важным деловым активам, имеет ценность для организации и, следовательно, должна быть защищена соответствующим образом. Конфиденциальность, целостность и доступность информации могут быть существенными аспектами для поддержания конкурентоспособности, денежного оборота, доходности, юридической гибкости и коммерческого имиджа. Информационная безопасность защищает информацию от широкого диапазона угроз как раз для того, чтобы обеспечить уверенность в непрерывности бизнеса, доведения до минимума ущерба, наносимого бизнесу, и доведения до максимума возвращения инвестиций и возможностей бизнеса.

Информационная безопасность достигается реализацией соответствующего множества средств управления, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Эти средства управления необходимо устанавливать таким образом, чтобы обеспечивать уверенность в том, что определенные цели безопасности организации достигнуты [1].

Данная курсовая работа посвящена анализу информационной системы отделения фонда социального страхования и по его результатам разработана спецификация требований, призванных обеспечивать руководство организации управлением и поддержкой информационной безопасности, т. е. политика информационной безопасности.

Курсовая работа состоит из 3 разделов.

В первом разделе происходит идентификация объектов защиты в информационной системе отделения фонда социального страхования.

Во втором разделе рассматриваются наиболее актуальные угрозы для информационных ресурсов отделения фонда социального страхования.

Третий раздел посвящён разработке политики информационной безопасности организации.

1 Идентификация объектов защиты в информационной системе фонда социального страхования

1.1 Цели и задачи фонда

1.1.1 Цель деятельности фонда социального страхования — обеспечение обязательного социального страхования граждан России.

1.1.2 Отделение фонда социального страхования осуществляет [2]:

- выплату пособий по временной нетрудоспособности;
- выплату пособий в связи с материнством и детством;
- обеспечение социальными пособиями на погребение;
- санаторно-курортное лечение. Оздоровление детей;
- финансирование проведения углубленных медицинских осмотров работников занятых на работах с вредными и (или) опасными производственными факторами.

1.1.3 Функции фонда, которые могут быть автоматизированы с помощью информационной системы:

а) организация банков данных по всем категориям страхователей;

б) ежеквартальный приём и выверка отчётных данных страхователей.

1.2 Идентификация информационных процессов

В соответствии с функцией а) пункта 1.1.3 можно идентифицировать следующие информационные процессы.

1.2.1 Физическое или юридическое лицо, желающее зарегистрироваться в качестве страхователя, отправляет с курьером (представителем страхователя) на бумажном носителе заявление на регистрацию, необходимые данные, а также документы, подтверждающие сферу деятельности и уплату всех соответствующих налогов.

Получателем данной информации является специалист подразделения фонда, ответственный за регистрацию страхователей.

1.2.2 На основе документов, предоставляемых физическим или юридическим лицом, желающим зарегистрироваться в качестве страхователя, специалист подразделения фонда, ответственного за регистрацию страхователей (оператор), заносит необходимую информацию в реестр (базу данных), добавляя к ней регистрационный номер и код подчиненности. После чего с документов снимаются копии, которые вместе с заявлением на регистрацию сдаются в архив. Подлинники документов возвращаются страхователю.

1.2.3 Оператор получает доступ к информации, предоставленной страхователем, но имеет право лишь на ввод её в базу данных. После того, как данные о страхователе будут сохранены и отправлены по ЛВС на сервер БД, единственным обладателем права доступа и модификации этих данных становится администратор БД. В последующем доступ к информации, хранящейся в БД, осуществляется через АРМ сотрудниками Фонда в соответствии с их должностными обязанностями.

1.2.4 Используемые программные приложения:

- программа для ввода данных о страхователе;
- СУБД;

– ОС.

1.2.5 Ввод информации осуществляется непосредственно на АРМ оператора, последующая обработка и модификация — на АРМ администратора баз данных.

Ввод данных с бумажных носителей в реестр, добавление регистрационного номера и кода подчиненности осуществляется оператором вручную.

1.2.6 Путь перемещения информации в ИС: АРМ оператора — коммутатор — маршрутизатор — сервер БД.

1.2.7 Обработанная информация в виде структурированной БД хранится на сервере БД, а также на сервере резервного копирования. Доступ к информации в БД осуществляется средствами запросов СУБД с АРМ сотрудников фонда в соответствии с их должностными полномочиями.

В соответствии с функцией б) пункта 1.1.3 можно идентифицировать следующие информационные процессы.

1.2.8 Отчётные данные поступают от страхователя с курьером (представителем страхователя) на бумажном носителе или через интернет (посредством электронной почты с использованием ЭЦП).

Отчёт исходит от бухгалтера страхователя к оператору ИС фонда.

1.2.9 Если отчёт поступает с курьером на бумажном носителе, специалист фонда (оператор) на своём рабочем месте осуществляет ручной ввод информации в базу данных (данные приводятся к формализованному виду), которая хранится на сервере баз данных. После чего отчёт сдается в архив.

1.2.10 Путь перемещения информации в ИС: АРМ оператора — коммутатор — маршрутизатор — сервер БД.

1.2.11 При получении отчёта по электронной почте на первом этапе администратор ИБ на своем АРМ производит проверку соответствующих реквизитов электронно-цифровой подписи. При подтверждении подлинности распаковывает сообщение с помощью программы-

упаковщика, в противном случае — уничтожает пакет.

Затем по внутренней ЛВС производит отправку полученных данных специалисту подразделения фонда, ответственного за бухгалтерский учёт и отчётность (оператору).

Оператор на своем АРМ осуществляет проверку правильности заполнения формы. В случае положительного результата проверки оператор производит добавление полученного отчёта к базе данных, хранящейся на сервере БД. В противном случае оператор посредством факса уведомляет отправителя, что его отчёт не принят, указав причину. После чего не принятый отчёт будет уничтожен.

1.2.12 Путь перемещения информации в ИС: почтовый сервер — АРМ администратора ИБ — коммутатор — АРМ оператора — коммутатор — маршрутизатор — сервер БД.

1.2.13 Администратор ИБ не имеет прав на модификацию информации. Оператор имеет доступ к данной информации, но имеет право лишь на ввод её в базу данных. После того, как отчёт будет сохранен и отправлен по ЛВС на сервер БД, единственным обладателем права их модификации становится администратор БД. В последующем доступ к информации, хранящейся в БД, осуществляется через АРМ сотрудниками фонда в соответствии с их должностными обязанностями.

1.2.14 Используемые программные приложения:

– программа для ввода данных отчёта;

– СУБД;

– программа-упаковщик;

– программа для проверки ЭЦП;

– ОС.

1.2.15 Отчётные данные страхователя заносятся в базу данных специалистом фонда или автоматически.

1.2.16 После обработки обработанная информация в виде структурированной БД хранится на сервере БД, а также на сервере резерв-

ного копирования. Доступ к информации в БД осуществляется средствами запросов СУБД с АРМ сотрудников фонда в соответствии с их должностными полномочиями.

1.2.17 Лицом, ответственным за функциональным состоянием аппаратных компонентов в ИС фонда социального страхования, является системный администратор.

1.3 Структура ИС фонда

1.3.1 Информационная система фонда состоит из следующих элементов:

а) серверная ферма:

1) почтовый сервер;
2) сервер обработки, на котором установлена СУБД;
3) сервер резервного копирования.

б) Автоматизированные рабочие места:

1) операторов;
2) администратора БД (резервного копирования);
3) администратора почтового сервера;
4) администратора ИБ.

в) Сетевое оборудование:

1) коммутатор;
2) маршрутизатор.

1.3.2 Графическое изображение конфигурации системы представлено на рисунке:

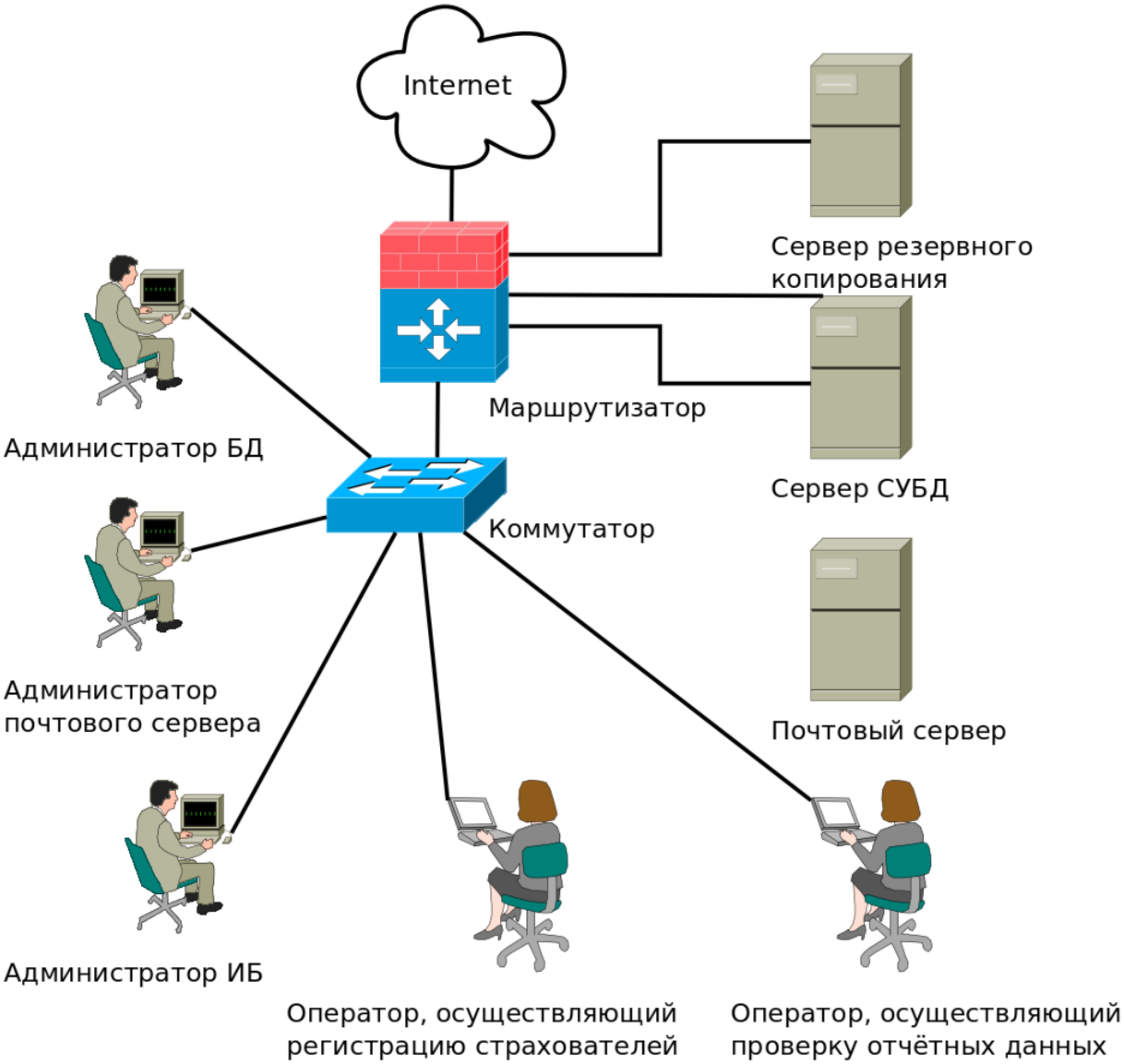

Рисунок 1.3.1 – Конфигурация информационной системы фонда социального страхования

1.4 Идентификация аппаратных ресурсов фонда как объектов защиты

1.4.1 Следующим этапом курсовой работы является определение ответственных за каждый аппаратный ресурс ИС и их полномочия по отношению к этим ресурсам с точки зрения возможности изменения конфигурации этих ресурсов. Для каждого аппаратного ресурса определяются его пользователи и их полномочия тоже с точки зрения

возможности изменения конфигурации этих ресурсов, т. е. происходит идентификация аппаратных ресурсов как объектов защиты с указанием возможных источников угроз для них.

1.4.2 Результат представлен в таблице A.1 Приложения A.

1.5 Идентификация информационных ресурсов фонда как объектов защиты

1.5.1 На следующем этапе курсовой работы необходимо идентифицировать информационные ресурсы, подлежащие защите.

1.5.2 В результате выполнения рабочих процессов организации образуются следующие информационные ресурсы:

- документы, необходимые для регистрации страхователя, поступившие с курьером;
- отчёт о работе страхователя, поступивший с курьером;
- отчёт о работе страхователя, поступивший электронной почтой;
- база данных.
- резервная копия базы данных;

1.5.3 В таблице 1.5.1 представлена классификация информационных ресурсов по степени критичности относительно доступности, целостности и конфиденциальности.

1.5.4 В таблице A.2 Приложения A определяются ответственные за информационные ресурсы фонда, их пользователи, а также как ответственные и пользователи используют информационные ресурсы.

Таблица 1.5.1 – Классификация ИР фонда по степени критичности

Информационный ресурс	Степень критичности информации		
	Доступность	Целостность	Конфиденциальность
Документы, необходимые для регистрации страхователя	Важная	Важная	Значимая
Отчётные данные страхователя на бумажном носителе	Важная	Важная	Значимая
Отчётные данные страхователя в электронном виде	Важная	Важная	Значимая
Содержимое сервера БД	Критическая	Критическая	Очень важная
Резервная копия БД	Важная	Очень важная	Очень важная

1.6 Схема информационных потоков в ИС фонда

На основе результатов предшествующего анализа на базе структуры ИС фонда разрабатывается схема информационных потоков в ИС фонда. Схема информационных потоков представлена на рисунке 1.6.1.

1 — отчётные данные страхователя в электронном виде;

2 — проверка реквизитор ЭЦП;

3 — перемещение отчёта после проверки ЭЦП;

4 — отчётные данные страхователя на бумажном носителе;

5 — запись отчёта в БД;

6 — документы, необходимые для регистрации страхователей;

7 — запись в БД данных о страхователях;

8 — просмотр и модификация БД;

9 — мониторинг состояния;

10 — резервная копия БД;

11 — откат БД с использованием резервной копии;

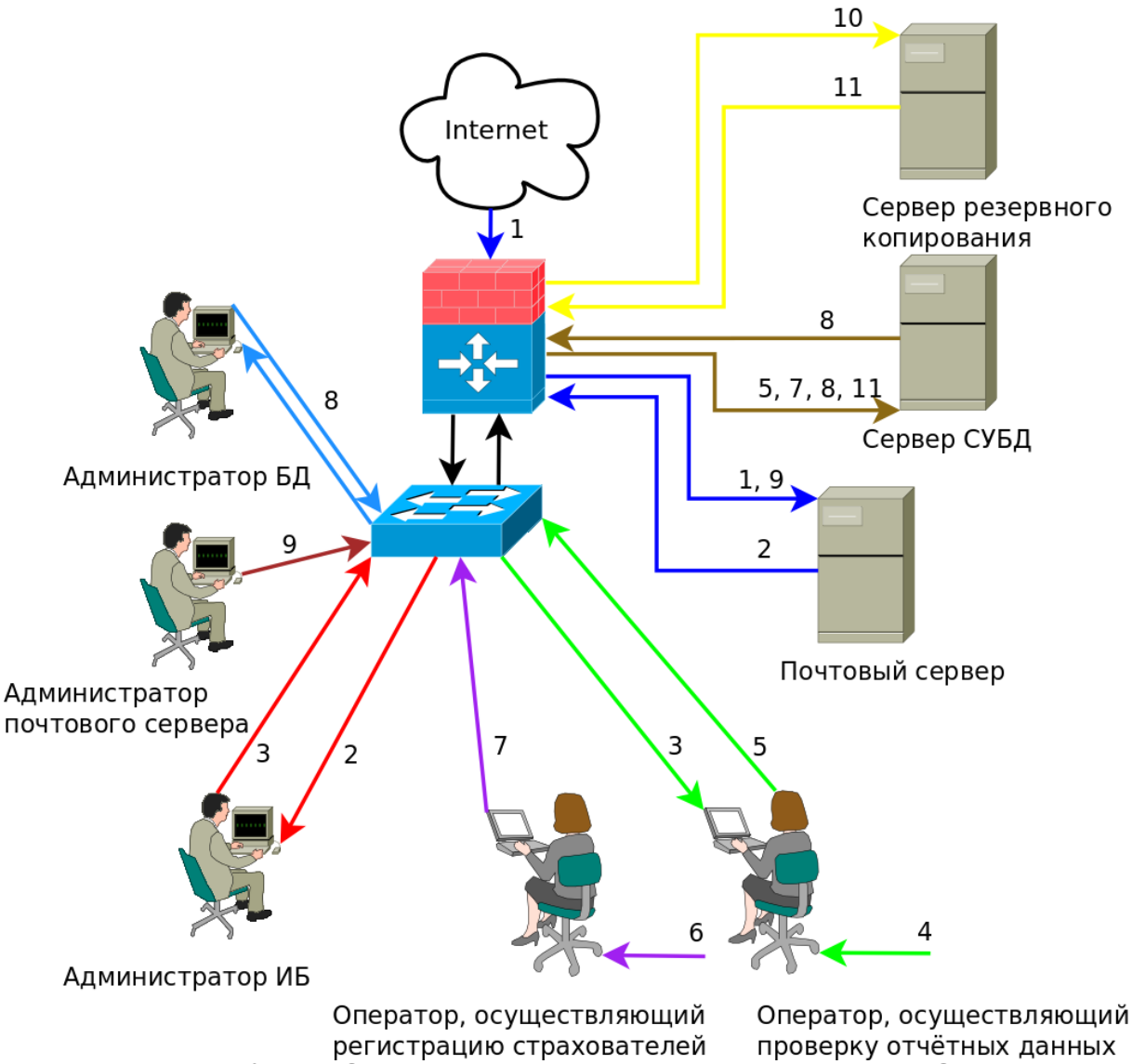

Рисунок 1.6.1 – Схема информационных потоков и ИС фонда

2 Идентификация актуальных угроз для информационных ресурсов отделения фонда социального страхования

2.1 Описание угроз защищаемым информационным ресурсам

2.1.1 Во второй части курсовой работы необходимо идентифицировать наиболее актуальные для информационных ресурсов фонда угрозы.

Разработка описания угроз защищаемым информационным ресурсам фонда осуществляется на основе модели угроз из национального стандарта ГОСТ Р ИСО/МЭК 15408.

2.1.2 Исходные перечень угроз:

- нарушение конфиденциальности защищаемой информации;
- нарушение целостности защищаемой информации.

2.1.3 Уровнями информационно-технологической инфраструктуры фонда, по которым следует локализовать каждый вид угроз из заданного перечня:

- уровень сетевых приложений, к которым можно отнести почтовые программные средства;
- уровень операционных систем.

Результат описания угроз приведён в таблице Б.1 приложения Б.

2.1.4 На уровне сетевых приложений можно выделить следующие угрозы:

– угроза внедрения в программу почтового сервера вредоносного кода;

– угроза утечки аутентификационных данных сотрудников фонда;

– угроза атаки на SSH-сервер;

– угроза атаки на программу почтового сервера.

2.1.5 На уровне операционных систем можно выделить следующие угрозы:

– угроза внедрения в ОС программы-вируса;

– угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ.

2.1.6 Угроза внедрения в программу почтового сервера вредоносного кода, описанная в таблице может быть реализована по следующим двум сценариям [3].

2.1.7 Злоумышленник, не имеющий отношения к отделению фонда, желает получить конфиденциальную информацию, содержащуюся в отчётных данных страхователей, для использования её в корыстных целях.

В связи с тем, что в отделении фонда социального страхования версии программного обеспечения обновляются недостаточно часто, злоумышленник может использовать ошибки его реализации, например, у некоторых серверов в файле `/etc/aliases` присутствует строка `decode: |/usr/bin/uudecode` автоматического запуска программы `uudecode` для распаковки сообщений `UUE`.

Многие расшифровщики помещают раскодированный текст в файл, указанный в заголовке `UUE`, допуская его перезапись без запроса подтверждения от пользователя. Если, как часто и бывает, почтовый сервер обладает наивысшими привилегиями, программа `uudecode` унаследует их при запуске, а злоумышленник получает возможность перезаписи любого файла в системе.

Например, он может внести в файл `/.forward` строку вида `oot, root@somehost.org` — для организации дублирования почты администратора на свой собственный адрес.

Далее начинает производиться несанкционированная пересылка писем, приходящих на почтовый сервер, посторонним лицам по Интернет, тем самым нарушается конфиденциальность важной информации. Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда в данном случае следует признать серьёзным.

2.1.8 Программист-злоумышленник, не имеющий отношения к отделению фонда социального страхования, обладающий детальными знаниями языков программирования и принципов работы антивирусных программ, достигший профессионального уровня в написании вредоносных программ-вирусов, с целью умышленного причинения вреда пользователям сети Интернет для повышения самооценки пишет новый компьютерный вирус, основанный на уязвимости в реализации почтового сервера, заключающейся в возможности выполнить код на почтовом сервере, используя неявную поддержку конвейера в полях `MAIL FROM` и `RCPT TO`.

Например, команда языка `Perl` может не только открывать файл, но и запускать его, если в имени присутствует символ «|», обозначающий вызов конвейера.

Уязвимость возникла из-за того, что версии программного обеспечения обновляются недостаточно часто.

С использованием ошибки переполнения буфера, вирус начинает модифицировать информацию в письмах, приходящих на почтовый сервер, тем самым нарушая целостность важной информации. Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры фонда в данном случае следует признать серьёзным;

2.1.9 Угроза утечки аутентификационных данных сотрудников фонда, описанная в таблице может быть реализована следующему сце-

нарию.

2.1.10 Администратор ИБ отделения фонда социального страхования, имеющий опыт работы высокого профессионального уровня, детально знающий принципы работы программы сервера баз данных, при отсутствии системы работы с персоналом в организации, попав в состояние нескорректированной вовремя психологической неустойчивости, возникшей из-за возможного увольнения за прогул, хочет отомстить руководству фонда.

Администратор ИБ, обладая всеми необходимыми средствами администрирования на своём рабочем месте, решает опубликовать в интернете пароли для доступа к почтовым ящикам всех сотрудников фонда Таким образом происходит нарушение конфиденциальности аутентификационной информации, которая может быть использована лицами, не имеющими отношения к отделению фонда, для осуществления НСД к письмам, приходящим на почтовый сервер отделения фонда социального страхования.

Возможность такого нападения маловероятна, но масштаб прямого ущерба для информационно-технологической инфраструктуры фонда следует признать серьёзным.

2.1.11 Угроза атаки на SSH-сервер, описанная в таблице может быть реализована по следующему сценарию.

2.1.12 Для доступа к почтовому серверу в отделении фонда используется безопасное соединение с использованием сетевого протокола SSH, позволяющий шифровать весь трафик, включая и передаваемые пароли.

Администратор ИБ, не обладая необходимыми знаниями, совершил ошибки в настройки SSH-сервера [4]:

- не запретил удалённый root-доступ;
- не изменил порт для доступа к SSH-серверу;
- не ограничил список IP-адресов, с которых разрешен доступ;
- использовал недостаточно надёжный пароль.

Таким образом, злоумышленник, не имеющий отношения к отделению фонда социального страхования, который может не обладать высоким знаниями в программировании и не знать деталей функционирования информационной системы фонда, получает возможность получить привилегию пользователя `root` на почтовом сервере. В результате этого может быть нарушена конфиденциальность и целостность критической для жизнедеятельности фонда информации — отчётных данных страхователей, хранимых на почтовом сервере.

Возможность такого нападения высока и масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда следует признать серьёзным.

2.1.13 Угроза атаки на программу почтового сервера, описанная в таблице может быть реализована по следующему сценарию.

2.1.14 Злоумышленник, не имеющий отношения к отделению фонда социального страхования, обладающий детальными знаниями языков программирования и принципов работы межсетевых экранов, а также имеющий большой опыт в их преодолении, с целью умышленного причинения вреда отделению фонда для повышения самооценки производит сканирование сетевых портов `TCP/UDP` серверов фонда с целью обнаружения незащищенных.

Мотивом данного действия служит возможность хищения конфиденциальной информации для использования её в корыстных целях. В связи с тем, что установленный в отделении фонда межсетевой экран не обеспечивает необходимую защиту, при сканировании компьютерный взломщик с легкостью обнаруживает незащищённые порты, после чего производит несанкционированное подключение к почтовому серверу отделения через Интернет и хищение конфиденциальной информации, находящейся в письмах, которые приходят по электронной почте. Таким образом происходит нарушение конфиденциальности важной информации. Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда социального страхования в данном случае следует

признать серьёзным.

Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда в данном случае следует признать серьёзным.

2.1.15 Угроза внедрения в ОС программы-вируса, описанная в таблице может быть реализована по следующим трём сценариям.

2.1.16 Создатели антивирусных программ, не имеющие отношения к отделению фонда социального страхования, являющиеся опытными программистами, достигшими профессионального уровня в написании программ-антивирусов, обладающие детальными знаниями языков программирования, с целью умышленного причинения вреда пользователям сети Интернет пишут новый компьютерный вирус, способный преодолеть существующие на текущий момент антивирусные защитные системы. Антивирусная программа создается параллельно с этим вирусом.

Мотивом данного действия является явная коммерческая выгода для создателей антивирусных программ, поскольку появление нового неизвестного вредоносного кода вынуждает пользователей сети Интернет покупать обновленные версии антивируса.

Ввиду того, что вирусные базы антивирусной программы в отделении фонда социального страхования обновляются недостаточно часто, вышеописанный вирус попадает в ИС фонда, после чего внедряется в системные и загрузочные файлы операционных систем, под управлением которых находится почтовый сервер и сервер БД. После внедрения вирус начинает изменять системные и загрузочные файлы ОС. В результате этого в процессе обработки происходит нарушение целостности БД, размещенной на сервере БД и отчётных данных страхователей, размещённых на почтовом сервере. Вероятность такого нападения высока. Масштаб прямого ущерба для информармационно-технологической инфраструктуры фонда в данном случае следует признать серьёзным;

2.1.17 Программист-злоумышленник, не имеющий отношения

к отделению фонда социального страхования, обладающий детальными знаниями языков программирования и принципов работы антивирусных программ, достигший профессионального уровня в написании вредоносных программ-вирусов, с целью умышленного причинения вреда пользователям сети Интернет для повышения самооценки пишет новый компьютерный вирус, способный преодолеть существующие на текущий момент антивирусные защитные системы.

Вирус, проявивший себя в сети Интернет, обнаруживается специалистами организаций, занимающихся разработкой антивирусных программ, после чего для антивирусных программ в короткий срок выпускаются очередные обновления, способные бороться с указанным вирусом.

Домашний компьютер администратора БД, не имеющий антивирусной защиты, заражается вирусом типа «`spyware`», копия вируса перезаписывается на флеш-накопитель администратора.

Администратор БД подключает флеш-накопитель на своём автоматизированном месте в отделении фонда социального страхования.

В связи с тем, что в отделении фонда вирусные базы антивирусной программы обновляются недостаточно часто, вирус проникает в ИС фонда, после чего внедряется в системные файлы операционных систем, под управлением которых находится сервер БД и почтовый сервер. После внедрения вирус начинает пересылку конфиденциальных данных о страхователях злоумышленнику. В результате этого в процессе обработки происходит нарушение конфиденциальности БД, размещенной на сервере БД, отчётных данных страхователей, размещённых на почтовом сервере. Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда в данном случае следует признать серьёзным.

2.1.18 Программист-злоумышленник, не имеющий отношения к отделению фонда социального страхования, обладающий детальными знаниями языков программирования и принципов работы анти-

вирусных программ, достигший профессионального уровня в написании вредоносных программ-вирусов, с целью умышленного причинения вреда пользователям сети Интернет для повышения самооценки пишет новый компьютерный вирус, способный преодолеть существующие на текущий момент антивирусные защитные системы.

Вирус, проявивший себя в сети Интернет, обнаруживается специалистами организаций, занимающихся разработкой антивирусных программ, после чего для антивирусных программ в короткий срок выпускаются очередные обновления, способные бороться с указанным вирусом. Но в связи с тем, что в отделении фонда вирусные базы антивирусной программы обновляются недостаточно часто, вирус проникает в ИС, после чего внедряется в системные и загрузочные файлы операционной системы, под управлением которой находится сервер БД. После внедрения вирус начинает изменять системные и загрузочные файлы ОС.

В результате этого в процессе обработки происходит нарушение целостности БД, размещенной на сервере БД. Вероятность такого нападения высока. Масштаб прямого ущерба для информационно-технологической инфраструктуры фонда в данном случае следует признать серьёзным.

2.1.19 Угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ, описанная в таблице может быть реализована по следующим двум сценариям.

2.1.20 Администратор ИБ фонда, имеющий опыт работы высокого профессионального уровня, детально знающий организацию операционной системы, применяемой в ИС, и её функционирование, при отсутствии системы работы с персоналом в организации, попав в состояние нескорректированной вовремя психологической неустойчивости, возникшей из-за возможного увольнения за прогул, хочет отомстить руководству фонда и для демонстрации значимости своей работы руководству решает умышленно нарушить целостность важной для ИС информации.

Используя как уязвимость доступность для редактирования системных файлов ОС сервера БД, администратор ИБ производит их некорректное редактирование.

В результате этого в процессе обработки происходит нарушение целостности БД, размещенной на сервере БД. Возможность такого нападения маловероятна, но масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда социального страхования следует признать серьёзным.

2.1.21 Администратор ИБ, имеющий опыт работы высокого профессионального уровня, детально знающий организацию операционной системы, применяемой в ИС, и её функционирование, ввиду сильного переутомления на рабочем месте, неумышленно производит некорректное редактирование системных файлов ОС сервера БД. В результате этого в процессе обработки происходит нарушение целостности БД, размещённой на сервере БД. Возможность такого нападения маловероятна, но масштаб прямого ущерба для информационно-технологической инфраструктуры отделения фонда социального страхования следует признать серьёзным.

2.2 Оценка рисков реализации угроз информационным ресурсам отделения фонда соцального страхования

2.2.1 Точный прогноз актуальных угроз позволяет снизить риск нарушения ИБ при минимизации затрат ресурсов организации. В процессе анализа возможных и выявления актуальных для активов организации угроз должен оцениваться риск, возникающий вследствие воздействия определенной угрозы.

2.2.2 Первым этапом была произведена оценка риска причинения вреда информационно-технологической инфраструктуре отделения

фонда социального страхования с учётом значений оценок возможностей реализации угрозы безопасности, а также значений масштабов ущерба, выявленных ранее при описании факторов угрозы.

2.2.3 На основе анализа возможности реализации каждой угрозы в сочетании с масштабом ущерба для информационно-технологической инфраструктуры, были выбраны определенные значения значимости риска с учётом приведенных в таблице 2.2.1. При этом были учтены результаты, полученные в процессе формирования описания ИС, угроз и сценариев реализации угроз на предыдущих этапах выполнения курсовой работы.

Таблица 2.2.1 – Значимость риска, исходя из сочетания возможности нападения и масштаба ущерба

Возможность нападения	Масштаб ущерба			
	Катастрофический — 4	Значительный — 3	Серьёзный — 2	Незначительный — 1
Частое — 6	24	18	12	6
Возможное — 5	20	15	10	5
Случайное — 4	16	12	8	4
Маловероятное — 3	12	9	6	3
Неправдоподобное — 2	8	6	4	2
Невозможное — 1	4	3	2	1

2.2.4 После этого полученное число для каждой угрозы было соотнесено с интервалом на качественной шкале, форма которой показана в таблице 2.2.2. Далее была составлена сводная таблица значимости риска реализации угроз с точки зрения нанесения ущерба информационно-технологической инфраструктуре, которая приведена в таблице 2.2.3.

Таблица 2.2.2 – Качественная шкала значимости риска реализации угрозы

Параметры	Интервалы шкал		
Балльные оценки	24-9	8-4	3-1
Качественные оценки	Высокая	Средняя	Низкая

Таблица 2.2.3 – Сводная таблица значимости риска реализации угроз для информационно-технологической инфраструктуры отделения фонда социального страхования

Угрозы по уровням инфраструктуры		Значимость риска реализации угроз	
		Балльная оценка	Качественная оценка
Уровень сетевых приложений	Угроза внедрения в программу почтового сервера вредоносного кода	12	В
	Угроза утечки аутентификационных данных сотрудников фонда	6	С
	Угроза атаки на SSH-сервер	12	В
	Угроза атаки на программу почтового сервера	12	В
Уровень операционных систем	Угроза внедрения в ОС программы-вируса	12	В
	Угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ	6	С

2.2.5 Вторым этапом оценки риска, является анализ влияния реализации угрозы на различные аспекты деятельности отделения фонда социального страхования. В отличие от оценки, даваемой на предыдущем этапе и связанной в основном с оценкой технических последствий реализации угрозы, на данном этапе во внимание принимается возможное влияние реализации угрозы на деятельность отделения фонда.

Матрица заполняется заданием уровня риска — высокого (В), среднего (С) или низкого (Н).

2.2.6 Оценка рисков реализации угроз на уровнях сетевых приложений и ОС инфраструктуры отделения фонда была проведена с помощью заполнения матрицы оценки риска.

2.2.7 Реализация угрозы нарушения целостности или конфиденциальности информации путем внедрения в программу почтового сервера вредоносного кода не приведет к серьёзным денежным потерям для отделения фонда социального страхования, соответственно уровень риска денежной потери следует принять низким. Уровень риска потери производительности в данном случае высокий, так как

нарушение целостности отчётов о работе страхователей, полученных программой почтового сервера, приведёт к некорректности результатов последующей работы фонда за длительный период времени, что в свою очередь приведёт к необходимости многократно повторять свои служебные обязанности персоналом отделения фонда. Уровень риска затруднения деятельности в данном случае также высокий, так как нарушение конфиденциальности отчётов о работе страхователей, полученных программой почтового сервера, приведёт к серьезного подрыву доверия страхователей к отделению фонда социального страхования.

2.2.8 Реализация угрозы нарушения конфиденциальности информации из-за утечки аутентификационных данных сотрудников фонда не приведет к серьёзным денежным потерям для отделения фонда, соответственно уровень риска денежной потери следует принять низким. Уровень риска потери производительности в данном случае также низкий, так как реализация данной угрозы не потребует дублирования усилий персонала отделения фонда и не приведёт к недоступности бизнес-функций. Уровень риска затруднения деятельности в данном случае следует принять высоким, так как нарушение конфиденциальности аутентификационных данных для подключения к `POP3`-серверу (`login`, `password`) может быть использовано лицами, не имеющими отношения к отделению фонда, для осуществления НСД к письмам, приходящим на почтовый сервер, что, в свою очередь, приведет к серьёзному подрыву доверия страхователей к отделению фонда.

2.2.9 Реализация угрозы нарушения целостности или конфиденциальности информации путем атаки на сервер `SSH` через Интернет не приведет к серьёзным денежным потерям для отделения фонда, соответственно уровень риска денежной потери следует принять низким. Уровень риска потери производительности в данном случае средний, так как нарушение целостности отчётов о работе страхователей, полученных программой почтового сервера, приведет к некорректности результатов последующей работы отделения фонда за короткий промежуток времени, что в свою очередь приведет к необходимости

продублировать работу сотрудников за это время. Уровень риска затруднения деятельности в данном случае следует принять высоким, так как нарушение конфиденциальности отчётов о работе страхователей, полученных программой почтового сервера, приведет к серьёзного подрыву доверия страхователей к отделению фонда.

2.2.10 Реализация угрозы нарушения конфиденциальности информации путем атаки на почтовый сервер через Интернет не приведет к серьёзным денежным потерям для отделения фонда, соответственно уровень риска денежной потери следует принять низким. Уровень риска потери производительности в данном случае также низкий, так как реализация данной угрозы не потребует дублирования усилий персонала отделения фонда и не приведёт к недоступности бизнес-функций. Уровень риска затруднения деятельности в данном случае следует принять высоким, так как нарушение конфиденциальности отчётов о работе страхователей, полученных программой почтового сервера, приведет к серьёзного подрыву доверия страхователей к отделению фонда.

2.2.11 Уровень риска денежной потери при реализации угрозы нарушения целостности или конфиденциальности информации путем внедрения в ОС программы-вируса следует принять средним, так как модификация системных и загрузочных файлов операционных систем, под управлением которых находятся АРМ и серверы, входящие в состав ИС, приведёт к невозможности дальнейшей работы данных ОС. Уровень риска потери производительности в данном случае высокий, так как нарушение целостности системных и загрузочных файлов операционных систем, под управлением которых находятся АРМ и серверы, входящие в состав ИС, к остановке их работы на длительный период времени. Уровень риска затруднения деятельности в данном случае следует принять низким, так как реализация данной угрозы не приведёт к подрыву общественного доверия к отделению фонда социального страхования.

2.2.12 Уровень риска денежной потери при реализации угрозы нарушения целостности информации путем уничтожения или некор-

ректной настройки критических файлов ОС администратором ИБ следует принять средним, так как модификация системных и загрузочных файлов операционных систем, под управлением которых находятся АРМ и серверы, входящие в состав ИС, приведёт к невозможности дальнейшей работы данных ОС. Уровень риска потери производительности в данном случае высокий, так как нарушение целостности системных и загрузочных файлов операционных систем, под управлением которых находятся АРМ и серверы, входящие в состав ИС, к остановке их работы на длительный период времени. Уровень риска затруднения деятельности в данном случае следует принять низким, так как реализация данной угрозы не приведет к подрыву общественного доверия к отделению фонда социального страхования.

2.2.13 Для определения общего риска нарушения деятельности организации от реализации каждой угрозы были использована таблица 2.2.4, а также качественная шкала из таблицы 2.2.2. Результат представлен в таблице Б.3 приложения Б.

Таблица 2.2.4 – Таблица для расчета общего риска нарушения деятельности

Риск денежной потери	Риск потери производительности								
	Низкий			Средний			Высокий		
	Риск затруднения деятельности			Риск затруднения деятельности			Риск затруднения деятельности		
	Н	С	В	Н	С	В	Н	С	В
Н	2	3	4	6	7	8	10	11	12
С	7	8	9	11	12	13	15	16	17
В	13	14	15	17	18	19	21	22	23

2.2.14 На третьем этапе было произведено определение комбинированного уровня риска для каждой угрозы и каждого уровня информационно-технологической инфраструктуры с помощью заполнения итоговой таблицы оценки риска.

2.2.15 Воспользовавшись таблицей 2.2.5, а также качественной шкалой из таблицы 2.2.2, была составлена итоговая таблица оценки риска. Результат представлен в таблице 2.2.6.

Таблица 2.2.5 – Таблица для расчёта итогового риска

Риск повреждения инфраструктуры	Риск нарушения деятельности		
	Низкий	Средний	Высокий
Низкий	2	8	16
Средний	5	10	19
Высокий	7	15	23

Таблица 2.2.6 – Итоговая таблица оценки риска реализации угроз

Угрозы по уровням инфраструктуры		Итоговая оценка риска реализации угроз	
		Балльная оценка	Качественная оценка
Уровень сетевых приложений	Угроза внедрения в программу почтового сервера вредоносного кода	23	В
	Угроза утечки аутентификационных данных сотрудников фонда	10	В
	Угроза атаки на SSH-сервер	15	В
	Угроза атаки на программу почтового сервера	15	В
Уровень ОС	Угроза внедрения в ОС программы-вируса	23	В
	Угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ	19	В

2.3 Определение перечня актуальных угроз информационным ресурсам отделения фонда социального страхования

На основе данных итоговой таблицы оценки рисков реализации угроз был сделан вывод, что все описанные угрозы являются актуальными для ИС отделения фонда социального страхования, то есть для реализации которых есть все необходимые условия (уязвимости, доступные ресурсы, масштаб ущерба и т.п.), и их реализация является эффективной для источника угроз по соотношению затраты/результат.

3 Разработка политики ИБ ИС отделения фонда социального страхования

3.1 Формулирование правил противодействия актуальным угрозам информационным ресурсам

3.1.1 На данной стадии выполнения курсовой работы была разработана политика информационной безопасности ИС отделения фонда социального страхования.

Первым шагом были сформулированы правила информационной безопасности отделения фонда социального страхования, составляющие основу политики безопасности.

3.1.2 Для отражения угрозы внедрения в программу почтового сервера вредоносного кода должны обеспечиваться:

- функционирование системы защиты автоматизированных рабочих мест и серверов ИС надежными антивирусными программными средствами, а также регулярное обновление их вирусных баз;
- регулярное обновление версий программного обеспечения;
- обеспечение обязательной проверки на наличие вирусов внешних носителей информации при подключении к ИС.

3.1.3 Для отражения угрозы утечки аутентификационных данных сотрудников фонда должны обеспечиваться:

- регистрировать действия администраторов в специальном журнале аудита;

– функционирование системы работы с персоналом с целью своевременного выявления и устранения причин неудовлетворенности условиями труда сотрудников.

3.1.4 Для отражения угрозы атаки на SSH-сервер должны обеспечиваться:

– функционирование системы защиты сетевых портов компьютеров, имеющих соединение с Интернет, программными или аппаратными межсетевыми экранами;
– организовать систему слежения, контроля состояния в работе сетевых программных приложений.

3.1.5 Для отражения угрозы атаки на почтовый сервер должно обеспечиваться функционирование системы защиты сетевых портов компьютеров, имеющих соединение с Интернет, программными или аппаратными межсетевыми экранами.

3.1.6 Для отражения угрозы внедрения в ОС программы-вируса в ИС должны обеспечиваться:

– функционирование системы защиты автоматизированных рабочих мест и серверов ИС надежными антивирусными программными средствами, а также регулярное обновление их вирусных баз;
– обеспечение обязательной проверки на наличие вирусов внешних носителей информации при подключении к ИС.

3.1.7 Для отражения угрозы уничтожения или некорректной настройки критических файлов ОС администратором ИБ должны обеспечиваться:

– функционирование системы обязательных перерывов на отдых для сотрудников, работа которых малоподвижна и требует высокой концентрации и внимания;

– функционирование системы работы с персоналом с целью своевременного выявления и устранения причин неудовлетворенности условиями труда сотрудников.

3.2 Формулирование политики ИБ ИС отделения фонда социального страхования

3.2.1 На втором этапе третьей стадии выполнения курсовой работы сформулированные ранее правила ИБ были взаимоувязаны в непрерывный по задачам, подсистемам и уровням комплекс — политику ИБ. Политика ИБ представляет собой совокупность правил и руководящих принципов в области ИБ, которыми руководствуется отделение фонда в своей деятельности. Результат представлен в таблице 16.

3.2.2 К основным принципам обеспечения ИБ в ИС отделения фонда относятся:

– системность;
– комплексность;
– непрерывная защита;
– разумная достаточность;
– гибкость управления и применения;
– открытость алгоритмов и механизмов защиты;
– простота применения защитных мер и средств.

Таблица 3.2.1 – Политика информационной безопасности ИС отделения фонда социального страхования

Правила ИБ	Руководящие принципы	Ответственный
Должно обеспечиваться функционирование системы защиты автоматизированных рабочих мест и серверов ИС надежными антивирусными программными средствами, а также регулярное обновление их вирусных баз, регулярное обновление версий программного обеспечения	Системность, непрерывная защита, открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств	Администратор ИБ
Должна обеспечиваться обязательная проверка на наличие вирусов внешних носителей информации при подключении к ИС	Системность, непрерывная защита, открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств	Администратор ИБ
Должно обеспечиваться функционирование системы обязательных перерывов на отдых для сотрудников фонда, работа которых малоподвижна и требует высокой концентрации и внимания	Системность, непрерывная защита, разумная достаточность	Начальник отдела охраны труда
Должно обеспечиваться функционирование системы работы с персоналом с целью своевременного выявления и устранения причин неудовлетворенности условиями труда сотрудников фонда	Системность, комплексность, непрерывная защита, разумная достаточность, гибкость применения	Начальник отдела охраны труда
Должно обеспечиваться функционирование системы защиты сетевых портов компьютеров, имеющих соединение с Интернет, программными или аппаратными межсетевыми экранами	Системность, комплексность, непрерывная защита, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты	Администратор ИБ

ЗАКЛЮЧЕНИЕ

В результате выполнения курсовой работы были получены навыки анализа угроз и разработки политики безопасности информационной системы организации на примере отделения Фонда социального страхования.

В процессе выполнения курсовой работы были описаны бизнес-функции отделения фонда социального страхования, структура и схема информационных потоков его информационной системы, а также угрозы ее безопасности и сценарии их реализации. Затем была произведена оценка рисков реализации угроз, на основе которой были выделены актуальные угрозы, после чего сформулированы правила информационной безопасности для противодействия этим угрозам. Последним этапом на основе сформулированных правил была разработана политика информационной безопасности информационной системы отделения Фонда социального страхования.

Задание на курсовое проектирование выполнено в полном объёме.

Список использованных источников

1. Сердюк В. А. Новое в защите от взлома корпоративных сетей — Москва: Техносфера, 2007. — 360 с.
2. Фонд социального страхования Российской Федерации [Электронный ресурс]: Положение о Фонде социального страхования — Режим доступа: http://www.fss.ru/ru/fund/about/fundamentals/6802.shtml.
3. Крис Касперски. Безопасность электронной почты // Журнал сетевых решений LAN — 10.10.2001 г. — http://www.osp.ru/lan/2001/05/135166/_p1.html.
4. SSH // Википедия. [2010—2010]. Дата обновления: 01.06.2010. URL: http://ru.wikipedia.org/?oldid=25053931 (дата обращения: 01.06.2010).

Приложение А

(обязательное)

Идентификация аппаратных и информационных ресурсов фонда как объектов защиты

Таблица А.1 – Идентификация аппаратных ресурсов фонда как объектов защиты

Аппаратный компонент	Ответственный	Полномочия ответственного	Пользователь	Полномочия пользователя
Сервер обработки	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов. Включение, выключение, перезагрузка сервера	Администратор БД	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Операторы фонда	Не имеют полномочий
Сервер резервного копирования	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов. Включение, выключение, перезагрузка сервера	Администратор БД	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Операторы фонда	Не имеют полномочий

Продолжение таблицы A.1

Аппаратный компонент	Ответственный	Полномочия ответственного	Пользователь	Полномочия пользователя
Почтовый сервер	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов. Включение, выключение, перезагрузка сервера	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Администратор ИБ	Подключение внешних носителей информации. Включение, выключение, перезагрузка сервера
			Операторы фонда	Не имеют полномочий
АРМ администратора БД	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Подключение внешних носителей информации
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации
			Операторы фонда	Не имеют полномочий
АРМ администратора почтового сервера	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Подключение внешних носителей информации
			Администратор ИБ	Подключение внешних носителей информации
			Операторы фонда	Не имеют полномочий

Продолжение таблицы A.1

Аппаратный компонент	Ответственный	Полномочия ответственного	Пользователь	Полномочия пользователя
АРМ администратора ИБ	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации
			Операторы фонда	Не имеют полномочий
АРМ регистрации страхователей	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации
			Операторы фонда	Включение и работа на ЭВМ
АРМ проверки отчётных данных	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Подключение внешних носителей информации
			Операторы фонда	Включение и работа на ЭВМ
Сетевое оборудование	Администратор ВС	Добавление, изменение, удаление аппаратных компонентов	Администратор БД	Не имеет полномочий
			Администратор почтового сервера	Не имеет полномочий
			Администратор ИБ	Не имеет полномочий
			Операторы фонда	Не имеют полномочий

Таблица А.2 – Идентификация информационных ресурсов фонда как объектов защиты

Информационный ресурс	Ответственный	Полномочия ответственного	Пользователь	Полномочия пользователя	Место хранения	Наибольшая защита
Документы, необходимые для регистрации страхователей	Оператор	Чтение, запись в БД	Оператор	Чтение запись в БД	Архив	Запись в БД
Отчётные данные страхователя на бумажном носителе	Оператор	Чтение, запись в БД	Оператор	Чтение запись в БД	Архив	Запись в БД
Отчётные данные страхователя в электронном виде	Оператор	Чтение, удаление, запись в БД	Оператор	Чтение, удаление, запись в БД	Сервер БД	Хранение в БД
			Администратор ИБ	Удаление		
Содержимое сервера БД	Администратор БД	Чтение, модификация, удаление	Оператор	Запись	Сервер БД	На всех этапах жизненного цикла
			Администратор ИБ	Чтение		
			Администратор БД	Чтение, модификация, удаление		
Резервная копия БД	Администратор БД	Чтение, удаление, запись	Администратор ИБ	Чтение, удаление, запись	Сервер резервного копирования	На всех этапах жизненного цикла
			Администратор БД	Чтение		

Приложение Б

(обязательное)

Оценка рисков реализации угроз информационным ресурсам отделения фонда социального страхования

Таблица Б.1 – Описание угроз

Угроза внедрения в программу почтового сервера программы-вируса Место локализации угрозы: почтовый сервер										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Несвоевременное обновление вирусных баз антивирусной программы, версий ПО; наличие уязвимости типа «buffer overflow» Зона локализации уязвимости: ПО, относящееся к среде эксплуатируемых систем	Частая	Несанкционированная пересылка вирусом отчетов посторонним лицам по Интернет	Отчёты о работе страхователей, полученные программой почтового сервера	Конфиденциальность	Серьёзный	Программист-злоумышленник, не имеющий отношения к фонду	Профессиональный уровень	Детальное знание принципов работы антивирусных программ; высокий уровень знания языков программирования	Персональный компьютер, наличие подключения к Интернет	Умышленное причинение вреда в корыстных целях
	Частая	Использование имеющейся уязвимости для искажения информации в письмах, приходящих на почтовый сервер	Отчёты о работе страхователей, полученные программой почтового сервера	Целостность	Серьёзный	Программист-злоумышленник, не имеющий отношения к отделению фонда	Профессиональный уровень	Детальное знание принципов работы антивирусных программ; высокий уровень знания языков программирования	Персональный компьютер, наличие подключения к Интернет	Умышленное причинение вреда для повышения самооценки

Продолжение таблицы Б.1

Угроза утечки аутентификационных данных сотрудников фонда Место локализации угрозы: почтовый сервер										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Отсутствие средств мониторинга за действиями администраторов. Зона локализации уязвимости: программное обеспечение, относящееся к среде эксплуатируемых систем и персонал ИС	Маловероятная	Администратор ИБ решает опубликовать в интернете пароли для доступа к почтовым ящикам всех сотрудников фонда	Отчёты о работе страхователей, полученные программой почтового сервера	Конфиденциальность	Серьёзный	Администратор ИБ	Профессиональный уровень	Детальное знание принципов работы программы почтового сервера	Не обязательны	Умышленное причинение вреда в целях мести

Продолжение таблицы Б.1

Угроза атаки на SSH-сервер Место локализации угрозы: почтовый сервер										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Некорректная настройка SSH-сервера. Зона локализации уязвимости: программное обеспечение, относящееся к среде эксплуатируемых систем	Частая	Несанкционированное подключение к почтовому серверу через Интернет и изменение информации в письмах, хищение конфиденциальной информации	Отчёты о работе страхователей, полученные программой почтового сервера	Конфиденциальность, целостность	Серьёзный	Компьютерный взломщик, пользователь сети Internet, не имеющий отношения к фонду	Не имеет значения	Хорошее знание принципов работы SSH-сервера	Персональный компьютер, наличие подключения к Интернет	Умышленное причинение вреда в для повышения самооценки

Продолжение таблицы Б.1

Угроза атаки на SSH-сервер Место локализации угрозы: почтовый сервер										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Некорректная настройка SSH-сервера. Зона локализации уязвимости: программное обеспечение, относящееся к среде эксплуатируемых систем	Частая	Несанкционированное подключение к почтовому серверу через Интернет и изменение информации в письмах, хищение конфиденциальной информации	Отчёты о работе страхователей, полученные программой почтового сервера	Конфиденциальность, целостность	Серьёзный	Компьютерный взломщик, пользователь сети Интернет, не имеющий отношения к фонду	Не имеет значения	Хорошее знание принципов работы SSH-сервера	Персональный компьютер, наличие подключения к Интернет	Умышленное причинение вреда в для повышения самооценки

Продолжение таблицы Б.1

Угроза внедрения в ОС программы-вируса Место локализации угрозы: автоматизированные рабочие места и серверы										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Несвоевременное обновление вирусных баз антивирусной программы. Зона локализации уязвимости: программное обеспечение, относящееся к среде эксплуатируемых систем	Частая	Изменение или уничтожение вирусом системных и загрузочных файлов ОС	Системные и загрузочные файлы операционных систем, под управлением которых находятся АРМ и серверы	Целостность	Серьёзный	Создатели антивирусной программы	Профессиональный уровень	Детальное знание принципов работы антивирусных программ; высокий уровень знания языков программирования	Штат опытных программистов; наличие подключения к Интернет	Коммерческая выгода
						Программист-злоумышленник, не имеющий отношения к фонду	Профессиональный уровень	Детальное знание принципов работы антивирусных программ; высокий уровень знания языков программирования	Персональный компьютер, наличие подключения к Интернет	Умышленное причинение вреда для повышения самооценки
		Получение НСД к информации путем использования программ типа «spyware»	Системные и загрузочные файлы операционных систем, под управлением которых находятся АРМ и серверы	Конфиденциальность	Серьёзный	Программист-злоумышленник, не имеющий отношения к фонду	Профессиональный уровень	Детальное знание принципов работы антивирусных программ; высокий уровень знания языков программирования	Персональный компьютер, наличие подключения к Интернет	Хищение информации для использования ее в корыстных целях

Продолжение таблицы Б.1

Угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ Место локализации угрозы: автоматизированные рабочие места и серверы										
Уязвимость	Возможность нападения	Метод нападения	Объект нападения	Тип потери	Масштаб ущерба	Источник угрозы	Опыт	Знание	Доступные ресурсы	Возможная мотивация действий
Доступность редактир-ния системных и загрузочных файлов (config.sys, boot.ini). Зона локализации уязвимости: персонал ИС и программное обеспечение, относящееся к среде эксплуатируемых систем	Маловероятная	Некорректное редактирование системных и загрузочных файлов и некорректное использование механизма восстановления ОС	Системные и загрузочные файлы операционных систем, под управлением которых находятся АРМ и серверы	Целостность	Серьёзный	Администратор ИБ	Профессиональный уровень	Детальное знание принципов работы антивирусных программ и сетевых приложений	Не обязательны	Умышленное причинение вреда в целях мести
										Неумышленное причинение вреда ввиду переутомления на рабочем месте

Таблица Б.3 – Матрица оценки рисков нарушения деятельности организации

Угрозы по уровням инфраструктуры		Риск денежной потери			Риск потери производительности			Риск затруднения деятельности			Общий риск		
Уровень сетевых приложений	Угроза внедрения в программу почтового сервера вредоносного кода			Н	В			В			В		
	Угроза утечки аутентификационных данных сотрудников фонда			Н			Н	В				С	
	Угроза атаки на SSH-сервер			Н		С		В				С	
	Угроза атаки на программу почтового сервера			Н			Н	В				С	
Уровень ОС	Угроза внедрения в ОС программы-вируса		С		В					Н	В		
	Угроза уничтожения или некорректной настройки критических файлов ОС администратором ИБ		С		В					Н	В		