УДК 004

Выбор политик и правил информационной безопасности для повышения уровня информационной защищенности центра оптовой торговли «Мост»

Ходич Д.В., Губенко Н. Е.
Донецкий национальный технический университет
Кафедра компьютерного моделирования и дизайна
dima_khodich@mail.ru, negubenko@mail.ru

Ходич Д.В., Губенко Н. Е. Выбор политик и правил информационной безопасности для повышения уровня информационной защищенности центра оптовой торговли «Мост». *В данной статье описан процесс и методы разработки политики информационной безопасности для ЦОТ "МОСТ".*

Ключевые слова: *Мост, центр оптовой торговли, информационная безопасность, разработка политик информационной безопасности, информационная защищённость*

.

Введение

Политика информационной безопасности ЦОТ «МОСТ» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Организация в своей деятельности.

Цели

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Задачами настоящей политики являются:

- описание системы управления информационной безопасностью в организации;
- определение политик информационной безопасности, а именно:
  - политика реализации антивирусной защиты;
  - политика учетных записей;
  - политика предоставления доступа к информационному ресурсу;
  - политика использования паролей;
  - политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС.

Построение структурной модели информационной системы (ИС)

Рассмотрим структуру центра оптовой торговли "МОСТ" с точки зрения информационной безопасности (ИБ). Структура включает в себя такие отделы и группы: отдел закупок, отдел менеджеров, отдел продаж, отдел складского хозяйства, отдел защиты информации, отдел режима и охраны, группа безопасности внешней политики и инженерно-техническая группа. Рассмотрим подробнее отделы, отвечающие за безопасность, представленные на рис. 1.

Рисунок 1 – Организационная структура ЦОТ “МОСТ”

Для того, чтобы можно было представить, как функционирует система, была составлена структурная модель ИС. Эта модель позволяет проанализировать функции, которые выполняются каждым звеном системы.

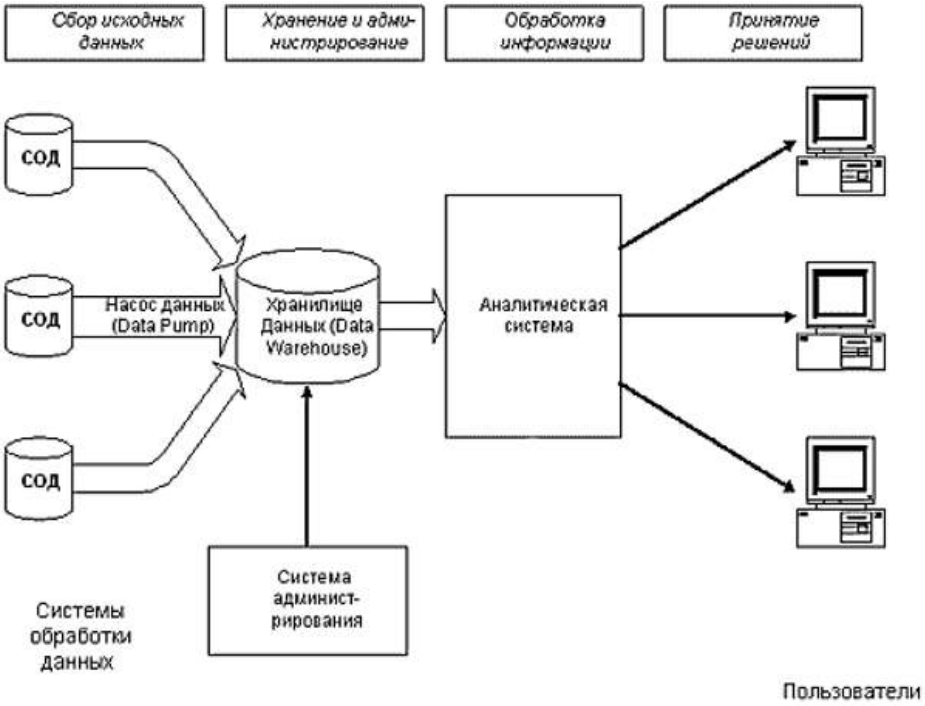

Рисунок 2 – Структурная модель информационной системы

После того как структура ИС определена нужно назначить ответственных за регламент использования каждого элемента системы для всех пользователей системы. В статье рассматривается определение полномочий

пользователей по отношению к компонентам ИС и проводится идентификация информационных ресурсов с точки зрения их критичности.

Классификация угроз ИБ для ЦОТ “МОСТ”

При проведении мониторинга структурной модели ИС были выявлены основные категории рисков, описанные в таблице 1.

Таблица 1 – Категории возможных потерь

Категории рисков	Описание
Риск потери ликвидности	Фирма не сможет в конкретный момент погасить свои обязательства имеющимся капиталом[1]
Потеря данных	К примеру потеря данных происходит тогда, когда персонал не выполняет своих обязанностей по политике безопасности предприятия.
Потеря рынка сбыта	Эта категория касается ситуаций, оказывающих влияние на установление общественного доверия.

Проведём оценку рисков. При этом уровни риска подразделяются на три категории: высокий (В), средний (С) и низкий (Н).

Таблица 2 – Матрица оценки рисков

Зона Уязвимости	Угроза	Риск потери ликвидности	Потеря данных	Потеря рынка сбыта
Физический Уровень	Неавторизованное раскрытие защищаемой информации	Н	В	С
	Ухудшение обслуживания	Н	Н	В
Сетевой Уровень	Неавторизованное раскрытие защищаемой информации	С	В	С
	Ухудшение обслуживания	Н	Н	В
Уровень СУБД	Неавторизованное раскрытие защищаемой информации	С	В	В
	Ухудшение обслуживания	Н	Н	В
Уровень бизнес-процессов организации	Неавторизованное раскрытие, защищаемой инф-ции	В	В	В
	Ухудшение обслуживания	С	С	В

Из таблицы 2 следует то, что актуальными угрозами, объектом атаки которых является информация, для организации являются: угроза неавторизованного раскрытия информации на сетевом уровне, на уровне СУБД, на уровне бизнес-процессов организации и угроза ухудшения обслуживания на уровне бизнес-процессов;

Разработка правил политики ИБ ЦОТ “МОСТ”

Политика информационной безопасности регламентирует эффективную работу средств защиты информации. Она охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика информационной безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты. [2]

В процессе разработки политики безопасности формулируется свод правил информационной безопасности для противодействия угрозам информационной системы организации. На основе свода правил создается политика безопасности.

Правило №1:

В данной организации должны отслеживаться действия пользователей и отправляться отчёты по собранной информации ответственным за регламент использования каждого компонента системы.

Правило №2:

Следует проводить модернизацию защиты информации и повышение квалификации персонала

Правило №3: Обеспечение защиты СУБД и хранение информации.

Правило №4: Обеспечение защиты бизнес-процессов ЦОТ “МОСТ”.

Правило №5: Разграничение доступа.

Правило №6: Использование современных инструментов защиты от вирусов.

Выводы

Описанные в тезисах методы для оценки риска, структурная модель и правила политики ИБ позволяют сформулировать политику безопасности ЦОТ «МОСТ» в виде следующей таблицы.

Таблица 3 – Политика безопасности организации

Правила ИБ	Ответственные	Виды защитных мер
В данной организации должны отслеживаться действия пользователей и отправляться отчёты по собранной информации ответственным за регламент использования каждого компонента системы.	Администратор ИБ	Организационные и технические
Следует проводить модернизацию защиты информации и повышение квалификации персонала в данной области	Администратор ИБ	Организационные
Обеспечение защиты СУБД и хранение информации	Персонал (операторы АРМ, администраторы)	Организационные и технические
Обеспечение защиты бизнес-процессов филиала коммерческого банка	Персонал (операторы АРМ, администраторы)	Организационные и технические
Разграничение доступа	Персонал (операторы АРМ, администраторы)	Организационные и технические
Использование современных инструментов защиты от вирусов.	Администраторы ИБ и СУБД	Организационные и технические

Требования настоящей Политики могут подчиняться и другим внутренними нормативными документами ЦОТ “МОСТ”, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также устава ЦОТ “МОСТ” настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также уставу ЦОТ “МОСТ”. В этом случае ответственное

подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

Ответственным за внесение изменений в настоящую Политику является руководитель структурного подразделения, по инициативе которого были внесены изменения.

Литература

1. Конфигурация "Учет мероприятий и семинаров"//Простой софт программы для дома и офиса. [Электронный ресурс]. – Режим доступа: http://www.aup.ru/articles/finance/4.htm

2.Конфигурация "Учет мероприятий и семинаров"//Простой софт программы для дома и офиса. [Электронный ресурс]. – Режим доступа: http://www.femida-audit.com/docs/038771.pdf

3. В.И. Ярочкин. Информационная безопасность. Учебник для вузов. – М.: Академический Проект, Мир, 2008. – 544 с.

4. Т.Л. Партыка, И.И. Попов. Информационная безопасность. – М.: Форум, Инфра-М, 2002.

5. В.П. Мельников, С.А. Клейменов, А.М. Петраков. Информационная безопасность. – М.: Академия, 2012. – 336 с.

6. В.И. Ярочкин, Я.В. Бузанова. Аудит безопасности фирмы: теория и практика. – М.: Академический проект, Парадигма, 2005. – 352 с.

7. С.Н. Загородников, А.А. Шмелев. Основы информационного права. – М.: Академический Проект, Парадигма, 2005. – 192 с.

8. А.Н. Прохода. Обеспечение интернет-безопасности. – М.: Горячая Линия - Телеком, 2007. – 184 с.

Ходич Д.В., Губенко Н. Е. Выбор политик и правил информационной безопасности для повышения уровня информационной защищенности центра оптовой торговли «Мост». *В данной статье описан процесс и методы разработки политики информационной безопасности для центра оптовой торговли “Мост”.*

Ключевые слова: *Мост, центр оптовой торговли, информационная безопасность, разработка политик информационной безопасности, информационная защищённость*

Khodich D., Gubenko N. The selection policies and rules of information security to enhance information security center of wholesale trade "Bridge". *This article describes the process and methods of developing information security policy for wholesale trading center “Bridge”*

Keywords: *Bridge, center of wholesale trade, information security, development of information security policies, information security.*