Министерство образования и науки российской федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Южно-Уральский государственный университет»
(Научно-исследовательский университет)
Факультет механико-технологический
Кафедра технологии автоматизированного машиностроения

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
технологии машиностроения,
д.т.н., профессор
_____ В.И. Гузеев
_____ 2017 г.

Совершенствование СМК путем разработки процесса информационная безопасность в соответствие с требованиями ИСО 27001

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–27.03.02.2017.1413 ПЗ ВКР

Консультанты
Экономическая часть,
д.т.н.. профессор
_____А.А. Николаенко
19.06 2017 г.

Менеджмента качества,
к.т.н., доцент
_____Н.В. Сырейщикова
16 июня 2017 г.

IDEF0 - моделирование,
к.т.н. профессор
_____П.П.Переверзев
16 июня 2017 г

Руководитель работы,
старший преподаватель
_____А.Х. Нуркенов
16.06. 2017 г.

Автор работы,
студент группы П-454
_____А.А. Фирсова
16.06. 2017 г.

Нормоконтролер,
к.т.н., доцент
_____А.В. Щурова
16 июня 2017 г.

Челябинск 2017

АННОТАЦИЯ

Фирсова А.А. Совершенствование СМК путем разработки процесса информационная безопасность в соответствие с требованиями ИСО 27001– Челябинск: ЮУрГУ П-454, 48 с., 6 рис., 6 табл., библиогр. список – 23 наименования, 3 приложения; альбом илл.16 л. ф.А4

Выпускная квалификационная работа (ВКР) выполнен с целью совершенствования процесса информационная безопасность в соответствие с требованиями ИСО 27001 для промышленного предприятия.

В ВКП проанализировано состояние дел на предприятии, выявлены проблемы предприятия, проведен анализ подходов к решению проблемы.

Усовершенствование процесса «Информационная безопасность» путем описания паспорта процесса, визуализации IDEF0 – моделями и разработкой оценочных показателе. Разработан менеджмент рисков для процесса «информационная безопасность». Рассчитан ожидаемый экономический эффект от результатов ВКР.

В работе использованы методы информационной безопасности: криптографический способ шифрования, протоколирование и аудит, межсетевое экранирование, создание резервных копий системы и документов; методы визуализации: IDEF0 – моделирование; методы менеджмента риска: анализ «галстук – бабочка», анализ видов и последствий отказов.

Результаты проекта имеют практическую ценность и внедрены на предприятие.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

> Любое решение надо основывать на таких принципах «можно ли реально снизить затраты?» и «поможет ли эта мера улучшить результаты всей компании?».
>
> Тайити Оно (исполнительный директор Toyota)

Актуальность темы. В настоящее время практически ни одна организация не обходится без использования информационных технологий. Данные, обрабатываемые в информационных системах, могут иметь высокую ценность для компании. В таких случаях становится неприемлемым нарушение тех или иных характеристик безопасности (конфиденциальности, целостности и доступности) критичной информации, поскольку это может привести не только к серьезному ущербу, но и поставить под сомнение дальнейшее существование предприятия. В связи с этим появляется необходимость в обеспечении защиты информации, обрабатываемой предприятием [1].

Понятие «информационная безопасность» сформировалось, когда люди стали пользоваться средствами информационных коммуникаций. На современном этапе сохранность конфиденциальности получаемой и передаваемой информации – это жизненно важный аспект [2].

На сегодняшний день угрозы и негативное воздействие на информационную систему безопасности предприятия происходит гарантировано при использовании сети Интернет, передачи информации с помощью информационных носителей и т.д., поэтому у руководителей предприятия появляется проблема обеспечения информационной безопасности информационных систем.

Основной целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию [3].

Цель и задачи ВКР

Цель выпускной квалификационной работы – совершенствование СМК путем разработки процесса информационная безопасность в соответствие с требованиями ИСО 27001.

Задачи работы:

1) провести анализ дел на предприятии;

2) сравнить отечественные и передовые зарубежные методы информационной безопасности;

3) усовершенствовать процесс информационная безопасность;

4) разработать методику «Информационная безопасность для условий предприятия»

5) определить экономическую эффективность результатов ВКР.

Объект проекта – процесс «Информационная безопасность»

Предмет проекта – методы оценки информационной безопасности.

1 АНАЛИЗ СОСТОЯНИЯ ДЕЛ НА ПРЕДПРИЯТИИ

1.1 О предприятии

1.1.2 История предприятия

Предприятие было зарегистрировано в октябре 1991 года. История становления предприятия началась с аренды производственных площадей с целью организации производства фланца и фланцевых крепежей.

За короткий период времени предприятие вышело в лидеры по производству фланцев в России, что послужило толчком для дальнейшего развития предприятия и уже в начале 20-х годов закрепляет за собой статус крупнейшего производителя фланцев в России – более 2000 тонн фланцев за год, а в 2004 году – 6000 тонн.

В начале 2004 года была сертифицирована система менеджмента качества в соответствии с требованиями MS ISO 9001, а уже в марте предприятие расширяет региональную сеть продаж в России – открытие представительства в Санкт-Петербурге .Далее было положено новое направление развития производства бугельных соединений для нефтяных платформ, их поставка в Италию для компании ,а также запуск горячештамповочного пресс-автомата HATEBUR-AMP20 для изготовления гайки М12-М24, организация производства шпиндельной пары Dy50 – 500 методом холодной накатки резьбы, не имеющей аналогов в России.

2009 год был насыщен значимыми событиями такие как: запуск горячештамповочного пресс-автомата HATEBUR-AMP30, формирование уникального горячештамповочного комплекса из двух пресс-автоматов, позволяющего изготавливать до 2,0 млн. шт. гайки в месяц М12 – М42. Но самым ярким событием 2009 года является регистрация исследовательского центра, в который входят 2 аккредитованные лаборатории: лаборатория неразруша-

ющего контроля (аттестована в 2009г) и лаборатория разрушающего контроля (аккредитована в 2010г).

В апреле 2016 года был одобрен премьер – министром РФ Дмитрием Медведевым проект по строительству, в индустриальном парке «Станкомаш», завода по производству высоковольтных двигателей АО «Русские электрические двигатели», что поспособствует к началу 2018 года локализировать производство электродвигателей для магистральных и подпорных насосных агрегатов для нефтедобывающей и нефтеперерабатывающей промышленности на территории Российской Федерации и уменьшить зависимость от иностранных производителей.

За время существования предприятия десятки тысяч его работников внесли огромный вклад в становление и развитие предприятия, благодаря их труду предприятие является ведущим в своей отрасли [22].

1.2 Номенклатура продукции

В настоящее время предприятие производит большое количество разнообразной продукции.

На предприятии представлен большой парк оборудования, позволяющий производить до 500 тонн фланцевой продукции в месяц, а также используется новейшие технологии, которые обеспечивают ряд технических преимуществ:

– плоские фланцы Ду15-500 штампуются на молотах и прессах;

– современная лаборатория;

– вертикально-фрезерный станок HARDINGE VMC 1000 II;

– электроэрозионный проволочновырезной станок CHMER CW-853HS и прошивной станок CHMER CM-323C+50NZ (изготовление сложного профиля инструмента).

Можно выделить несколько моделей фланцев, производимых на «Конаре»: фланцы воротниковые ГОСТ Р 54432-2011 (ГОСТ 12821-80) DN 16-1200, PN 1-25,0 Мпа; фланцы плоские ГОСТ Р 54432-2011 (ГОСТ 12820-80)

DN15-1400 PN1-2,5 Мпа; фланцы стальные по DIN-EN.1092-1и многие другие. На рисунке 1 представлен фланец воротниковый ГОСТ Р 54432-2011 (ГОСТ 12821-80) DN 16-1200, PN 1-25,0 Мпа.

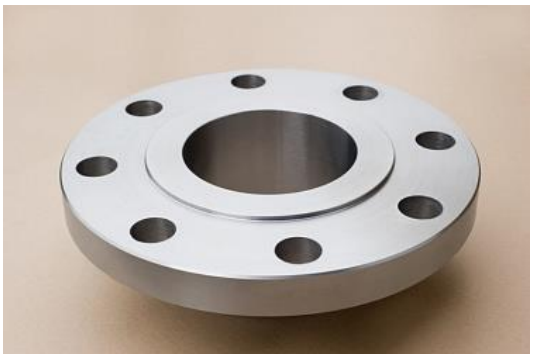


Рисунок 1 – фланец воротниковый ГОСТ Р 54432-2011 (ГОСТ 12821-80) DN 16-1200, PN 1-25,0 Мпа

Компания «Конар» производит несколько видов прокладок, условно их делят: металлические, неметаллические, комбинированные.

На рисунке 2 представлена шиберная стальная задвижка , которая относятся к запорной арматуре, а также служат для перекрытия потока рабочей среды, на технологических трубопроводах и объектах литейной части магистральных нефтепроводов, отвечают требованиям: ОТТ – 23.060.30 – КТН - 246-08, ГОСТ 5762, СНиП 2.05.06-85, ГОСТ 30546.1-98, ПБ 03-585-03.

Рисунок 2 – Шиберная стальная задвижка

Для клиновых и шиберных задвижек по чертежам производится шпиндельная пара осуществляющая передачу крутящего момента от привода к запирающему или регулирующему элементу арматуры и она должна иметь следующие основные элементы: участок трапециевидной ходовой резьбы, гладкий цилиндрический сальниковый участок, устройства для соединения шпинделя с запирающим элементом и с приводом. На рисунке 3 представлен шпиндель.

Рисунок 3 – Шпиндель

Специалистами инженерного центра разработаны вантузы нефтепровода ТУ 3663 – 001 – 21483089 – 2009, которые прошли экспертизу в ООО «НИИ ТНН», тем самым подтвердив высокий уровень и качество изделия. На рисунке 4 представлены вантузы трубопровода.

Вантузы нефтепроводов предназначены для впуска воздуха при освобождении и выпуска при заполнении нефтепровода нефтью, подключения насосных агрегатов, обеспечения откачки (закачки) нефти в период выполнения плановых, ремонтных работ на линейной части магистрального нефтепровода.

Рисунок 4 - Вантузы нефтепровода

Большая собственная производственная база, высококвалифицированные опытные сотрудники, наличие новейших лаборатории и инженерного центра позволили компании изготавливать изделия любой сложности и конфигурации по чертежам заказчика, например: камера для уровнемера, узел отбора давления на трубопроводах, фильтр пусковой тройниковый, фильтр сетчатый временный, фильтр V(T)- образный и т.д.

1.3 Реестр процессов и схема их взаимодействия

Основные процессы СМК, действующие на предприятии, и описание их взаимодействия приведены в Руководстве по качеству и в паспортах процессов. Схема взаимодействия процессов представлена в приложении А.

Руководство предприятия совместно с руководителями и специалистами подразделений определило процессы, необходимые для СМК и их применение на предприятии. Это процессы:

– управления;

– менеджмент продаж. Анализ и изучение требований потребителей;

– проектирование и модернизация изделий

– планирование;

– подготовка производства

– закупки;

– производство продукции;

– хранение и поставка;

– вспомогательные процессы, включающие в себя процессы менеджмента ресурсов и процессы измерения.

У процессов определены их владельцы и руководители. Функциям владельцев процессов:

1) определение целей;

2) постановка задач;

3) планирование мероприятий;

4) обеспечение ресурсами;

5) оценка результативности процесса;

6) принятие решений об изменениях.

7) организация выполнения всех необходимых действий в соответствии с запланированными мероприятиями в рамках выделенных ресурсов;

8) контроль и сбор данных для оценки результативности процесса.

Допустимые значения показателей результативности процессов установлены в паспортах процессов [6].

1.4 Система менеджмента качества

Система менеджмента качества разработана и внедрена по решению Генерального директора предприятия.

При разработке системы учитывались:

– состояние внешней среды, её изменения и риски связанные с этими изменениями;

– состояние внутренней среды предприятия и её изменения, связанные с изменением стратегии развития;

– принципы менеджмента качества;

– возможности улучшения СМК и её процессов путём применения цикла «PDCA».

Система менеджмента качества применяется для решения следующих задач:

– повышение удовлетворенности потребителей посредством обеспечения соответствия продукции требованиям и ожиданиям потребителей;

– реализация основных направлений, определенных Политикой в области качества;

– постоянного улучшения и повышение результативности СМК и её процессов.

В копании разработана, внедрена и поддерживается в рабочем состоянии система менеджмента качества в соответствии с требованиями международного стандарта ИСО 9001, которая является частью общей системы управления предприятием. Копия сертификата приведена в приложении В.

Руководство по качеству является основным документом системы менеджмента качества и используется в целях:

– определения процессов системы менеджмента качества и требований к ним;

– описания и внедрения системы менеджмента качества;

– представления системы менеджмента качества заказчику;

– обеспечения улучшения управления процессами;

– обучения персонала предприятия требованиям СМК;

– обеспечения документированной базы для проведения внутренних аудитов;

– предъявления системы менеджмента качества инспектирующему и сертифицирующему органу;

– реализации политики в области качества, процессов, процедур и требований;

– демонстрации соответствия системы качества требованиям к качеству в контрактных ситуациях.

Для обеспечения управляемости деятельностью и процессами, перед ними ставятся ежегодные цели, осуществляется планирование деятельности по достижению этих целей, мониторинг запланированной деятельности, проводится оценка результатов деятельности и сравнение их с поставленными

целями, проводится анализ, по результатам которого разрабатываются корректирующие действия.

Для поддержки этих процессов и их мониторинга выделяются необходимые ресурсы и информация. На основе анализа деятельности принимаются меры, необходимые для достижения запланированных результатов и улучшения процессов.

Основные цели и задачи по совершенствованию системы менеджмента качества изложены в «Политике в области качества и охраны окружающей среды» [6].

1.5 Диагностика проблем предприятия

Наиболее актуальной проблемой является нарушение информационной безопасности предприятия, ее можно разделить на следующие ключевые направления:

1) разглашение информации третьим лицам, может произойти из-за некомпетентности сотрудников, которые не выполняют правила защиты информации, ее могут передать с помощью сообщения, публикации, пересылки, утери, средств массовой информации, переписки, конференции, личные встречи;

2) несанкционированный доступ к информации, например передача конфиденциальной информации лицам, не обладающим правами доступа к ней; Условия способствующие завладению информацией считают: подкуп, плохую работу сотрудников, низкую заработную плату, отсутствие дисциплины и т.д;

3) низкая квалификация специалистов по защите информации может создать препятствия в создании защиты информационной безопасности предприятия;

4) низкий уровень исполнения намеченных целей по созданию системы защиты информации. Такая ситуация часто встречается на предприятиях,

когда намеченные цели и задачи теряются на уровне исполнения из-за недостаточной заинтересованности исполнителя, бюрократии;

5) отсутствие понимания у сотрудников важности проведения работ по защите информации. Персонал недостаточно информирован о целях и задачах предприятия и не понимает важности защиты конфиденциальных данных;

6) проблема политического характера, связанная с электронной разведкой, сетевымивойнами и в интересах государственной тайны, необходима защита информации от атак.

Цели и задачи проектирования

Согласно пункту ИСО 9001 «Менеджмент ресурсов» существует следующая классификация ресурсов: человеческие ресурсы, персонал, поставщики и партнеры, инфраструктура, производственная среда, информационные ресурсы, природные ресурсы [7]. Связующим этих ресурсов является информация, которая имеется в каждом из направлений классификации. Большой объем и эффективное управление с данными потоками информации представляет собой трудную задачу. Таким образом, управление потоками информации должно обеспечивать требования по безопасности согласно ГОСТ Р ИСО/МЭК 27001[8].

Выводы по разделу один

1) предприятие активно развивается и характеризуется широкой номенклатурой выпускаемых изделий и обладает необходимыми ресурсами для развития;
2) предприятие имеет действующее СМК, которое обеспечивает эффективное взаимодействие процессов и позволяет выполнять требования по качеству продукции и услуг;
3) в связи с обработкой большого объема информации и динамикой развития предприятия формируется потребность в постоянном совершенствовании процессов управления ресурсами. Согласно

СМК, ключевым ресурсом в «Менеджменте ресурсов» является информация [7]. Таким образом, совершенствование системы управления информационной безопасностью является приоритетным направлением.

В связи с актуальностью, целью работы является разработка методики «Информационная безопасность для условий АО «Конар»

Задачи для достижения этой цели:

1) провести анализ дел на предприятии;

2) сравнить отечественные и зарубежные методы информационной безопасности;

3) усовершенствовать процесс «Информационная безопасность»;

4) разработать методику «Информационная безопасность для условий предприятия»;

5) определить экономическую эффективность результатов ВКР.

2 СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ И ПЕРЕДОВЫХ ЗАРУБЕЖНЫХ МЕТОДОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном обществе информация является очень ценным ресурсом в любой деятельности человека. Поэтому каждое предприятие заинтересованно в своей информационной безопасности.

Успех предпринимательской деятельности в немалой степени зависит от умения распоряжаться таким ценнейшим товаром, как информация. Сейчас главным ресурсом вместо капитала становится именно информация.

Современные методы защиты данных нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

2.1 Криптографический способ шифрования

Криптография, или криптология, наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать без специального секретного ключа. В отечественном словоупотреблении термин «криптология» объединяет в себе «криптографию», т.е. шифрование сообщений, и «криптоанализ», т.е. несанкционированное расшифровывание сообщений. Исходное сообщение называется в криптографии открытым текстом, или клером. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или криптограммой. Процедура шифрования обычно включает в себя использование определенного алгоритма и ключа. Алгоритм – это определенный способ засекречивания сообщения, например компьютерная программа или, скажем, список инструкций. Ключ же конкретизирует процедуру засекречивания .

Современные методы криптографического преобразования информации могут быть разделены на 4 раздела: симметричные криптосистемы, криптосистемы с открытым ключом, электронная подпись, управление ключами.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответству-

ющего ему открытого текста, должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты;

– незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

– длина шифрованного текста должна быть равной длине исходного текста;

– не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Под симметричной криптосистемой понимается процесс шифрования или дешифрования, в котором используется один и тот же ключ. Исходный текст заменяется шифрованным текстом и на основе ключа шифрованный текст можно преобразовать в исходный.

Симметричные криптосистемы делятся на 4 класса преобразований:

1) подстановка – символы исходного шифруемого текста, заменяются на символы такого же или другого алфавита в соответствии с заранее определенными правилами;
2) перестановка – символы переставляются, в определенном пределе заданного блока передаваемого текста;
3) аналитическое преобразование – преобразование шифруемого текста по заданному аналитическому правилу;
4) комбинированное преобразование – последовательность преобразований, применяемая к части шифруемого текста.

В криптосистемах с открытым ключом используются два ключа (открытый, закрытый), которые связаны друг с другом математически. Шифрование информации, которая имеет общий доступ, происходит с помощью открытого ключа, а расшифровывание с помощью закрытого ключа, известного только получателю сообщения.

Существуют два требования к системам с открытым ключом:

1) изменение текста должно быть необратимым и не подлежащим восстановлению на основе открытого ключа;
2) определение закрытого ключа на основе открытого должно быть невозможным, при этом необходима низкая сложность расшифрования

Криптосистемы с открытым ключом также можно использовать, как самостоятельные средства защиты хранимых и передаваемых данных, а также как средства распределения ключей.

Электронная подпись – это присоединяемое к тексту криптографическое преобразование, которое позволяет при получении информации другим пользователем проверить авторство и подлинность [9].

Криптосистема основана на использовании ключей, поэтому проблема управления ключами актуальна.

Управление ключами является информационным процессом и включает в себя:

1) генерацию ключей – в сложных информационных системах используют специальные аппаратные и программные методы генерации, например датчики псевдослучайных чисел или устройства на основе «натуральных» случайных процессов.
2) накопление ключей – это хранение, учет и удаление ключей.
3) распределение ключей происходит двумя путями: создания одного или нескольких центров распределения ключей и прямой обмен ключами между пользователями информационной системы

Реализация криптографических методов

Проблема реализации методов защиты информации имеет два аспекта:

– разработку средств, реализующих криптографические алгоритмы;

– методику использования этих средств.

Каждый из рассмотренных криптографических методов могут быть реализованы либо программным, либо аппаратным способом. Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры. При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы. Большинство зарубежных серийных средств шифрования основано на американском стандарте DES. Отечественные же разработки, такие как, например, устройство КРИПТОН, использует отечественный стандарт шифрования. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз). В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеоб-

разный «криптографический сопроцессор» - вычислительное устройство, ориентированное на выполнение криптографических операций. Такой метод объединяет в себе достоинства программных и аппаратных методов [12].

2.2 Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационных системах.

Аудит – это анализ накопленной информации, проводимый в реальном времени или периодически. Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным [10].

Реализация протоколирования и аудита решает следующие задачи:

– обеспечение подотчетности пользователей и администраторов; является сдерживающим средством;

– обеспечение возможности реконструкции последовательности событий – позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе;

– обнаружение попыток нарушений информационной безопасности;

– предоставление информации для выявления и анализа проблем.

Для реализации эффективного протоколирование требуется определиться с тем, какие события регистрировать и с какой степенью детализации. Слишком обширное или подробное протоколирование не только снижает производительность работы ИС (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Основные события, безусловно требующие протоколирования:

– попытка входа в систему (успешная или нет);

– выход из системы;

– обращение к удаленной системе;

– операции с файлами (открыть, закрыть, переименовать, удалить);

– смена привилегий или иных атрибутов безопасности.

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

– дата и время события;

– уникальный идентификатор пользователя – инициатора действия;

– тип события;

– результат действия (успех или неудача);

– источник запроса (например, имя терминала);

– имена затронутых объектов (например, открываемых или удаляемых файлов);

– описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

В отношении определенной категории пользователей и событий может применяться выборочное протоколирование.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Обеспечение подотчетности важно, в первую очередь, как сдерживающее средство. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым защищается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе [13].

Реализация протоколирования и аудита в распределенной разнородной системе является сложной задачей по двум причинам:

– некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования, их нужно экранировать другими элементами, которые могут реализовать функции протоколирования,

– необходимо увязывать между собой события в разных элементах системы.

2.3 Межсетевое экранирование

Межсетевой экран – аппаратные и программные средства защиты сетей, которые предназначены для защиты компьютерных сетей или отдельных узлов как от несанкционированного доступа (НСД) к ним, так и от НСД из защищаемых узлов и сетей в сети общего пользования. Межсетевой экран осуществляет контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными политиками безопасности.

Сетевые технологии уже давно стали необходимым инструментом функционирования и развития бизнеса почти любого предприятия. Развитие корпоративных сетей, использование Интернета в коммерческих целях и для передачи информации между удалёнными филиалами – с одной стороны повышает эффективность бизнеса, а с другой – создаёт реальные и достаточно серьёзные риски информационной безопасности.

Внедрение системы межсетевого экранирования является одной из важнейших задач комплекса мероприятий по защите информационной среды предприятия. Система межсетевого экранирования делит сетевую инфраструктуру предприятия на сегменты и позволяет регламентировать доступ к

ним внутренних и внешних пользователей, обеспечивая детальный контроль над сетевыми потоками. Внедрение такой системы позволяет:

– ограничить возможности проведения атак на элементы сетевой инфраструктуры и программное обеспечение;

– ограничить возможность получения несанкционированного доступа к информационным системам и сервисам предприятия;

– изолировать возможные неприятные последствия инцидентов;

– собрать детальную информацию о возможных инцидентах для последующего анализа.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно – аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

– по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;

– по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Построение системы межсетевого экранирования позволит компаниям предотвратить угрозы и снизить риски информационной безопасности[11].

2.4 Создание резервных копий системы и документов

Обеспечение сохранности конфиденциальной информации, принадлежащей компании или частному лицу, становится первоочередной задачей для IT-технологий. Эффективно работающие системы сохранения дополнительных копий с переносом их на сменные накопители, дают возможность сократить ущерб от возможного исчезновения информационных файлов, что чаще всего происходит по следующим причинам:

– аппаратного характера;

– программно-логического характера, что вызывается проникновением вирусов в устройство, ошибками в структуре софта, отсутствием должной квалификации у пользователя.

Создание резервной копии, а именно так называют дублирование базы данных, информационных файлов, с последующим переносом дубликатов на сменные носители, дает возможность восстановить утраченные сведения при повреждении оригинала. На данный момент применяются следующие варианты резервного копирования:

– полный, затрагивающий всю систему, проводимый еженедельно;

– добавочный, что предусматривает создание копий только тех файлов, которые были изменены с момента предыдущего копирования;

– дифференциальный, затрагивающий лишь измененные файлы, благодаря чему откат после сбоя, аварийного завершения работы устройства, проводится быстрее.

В качестве методов дублирования важных информационных файлов используются:

– пофайловый, что предполагает сокращение затрат на его проведение, но невозможность использования в крупных организациях, где задействован не один сервер;

– отображающий, когда делается «снимок», благодаря чему ускоряются работа по восстановлению утраченной информации.

Анализ эффективности мероприятий, применяемых для предотвращения утраты важной информации, позволяет выделить следующие преимущества грамотно созданной системы резервного дублирования:

1 большая скорость восстановления утраченных данных, возможность выбора оптимального способа:

– мгновенное воспроизведение отдельных файлов;

– воссоздание всей программной системы за несколько минут;

– восстановление приложений, сделанных предварительно «образов» систем хранения информации;

– реставрация системы администрирования базы данных;

2 защита информации осуществляется непрерывно, послеаварийное ее восстановление оптимизировано для используемых бизнес-процессов:

– стратегия долгосрочного хранения сведений соответствует архивации данных на носителях с магнитной лентой;

– резервные «снимки» всей виртуальной машины значительно повышают возможности репликации;

– все запасные копии быстро и безопасно архивируются.

3 полноценно проведенное резервное дублирование гарантирует полное восстановление любого информационного файла:

– появляется возможность смоделировать воссоздание каждой успешно осуществленной резервной копии;

– восстановления сведений в любой выбранной точке становится реальностью.

4 существование резервных копий обеспечивает возможность создания виртуальной структуры предприятия:

– виртуальная модель создается практически моментально, а приложения запускаются из имеющихся копий;

– не затрагивая всю IT-инфраструктуру компании можно выявить функциональные проблемы в одной либо нескольких программно-аппаратных системах.

5 появляется возможность осуществлять постоянный мониторинг функциональности информационной системы предприятия, выявляя неисправности до момента их явного проявления:

– о любом снижении производительности оборудования, даже небольших проблемах, с которыми сталкивается дублирование информации, становится известно до начала сбоя в работе утилитов, явном нарушении функциональности устройства пользователя;

– потребитель получает возможность планировать использование собственных IT-ресурсов, что обеспечивает их оптимальное использование;

– системы резервного дублирования и реставрации информационных файлов предполагают создание отчетов по устанавливаемым стандартам, что облегчает проверку соответствия документов требованиям законодательства, упрощает проведение аудита.

Многофункциональность разработанных систем резервного копирования сведений и их восстановления позволяет минимизировать риски утраты данных, расширяет возможности эффективного управления бизнесом.

Технологии резервного копирования и восстановления не только решают задачи защиты данных, но и помогают существенно сэкономить время и финансовые расходы на восстановление работоспособности информационной инфраструктуры в случае форс-мажорных ситуаций [14].

Смена рабочего набора носителей в процессе копирования называется их ротацией. Для резервного копирования очень важным вопросом является выбор подходящей схемы ротации носителей (например, магнитных лент).

Таблица 1 – Сравнение методов информационной безопасности

Метод	Достоинства	Недостатки
Криптографический метод	Быстрая реализация. Высокая степень защиты информации.	Криптографическое преобразование информации занимает большое количество времени

Окончание таблицы 1

Протоколирование и аудит	Предоставление информации для выявления проблем. Обнаружение попыток нарушения ИБ	Может снизить производительность сервисов
Межсетевое экранирование	Повышение безопасности объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды	Уязвимость при подмене IP-адресов
Создание резервных копии системы и документов	Возможность экстренного восстановления данных, защита от утраты баз данных, корпоративной почты и другой информации.	Сложность в управлении резервными копиями, человеческий фактор

Выводы по разделу два

В разделе два проведено сравнение и сопоставление методов информационной безопасности, таких как

– криптографические методы;

– протоколирование и аудит;

– правовые методы;

– межсетевое экранирование;

– создание резервных копий системы и документов.

Проведен анализ методов, а также выявлены достоинства и недостатки каждого метода. Для надежной работы информационных систем предприятия рекомендуется применить метод протоколирование и аудит.

3 СОВЕРШЕНСТОВАНИЕ ПРОЦЕССА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

3.1 Процесс «информационная безопасность»

На основе стандарта ИСО/МЭК 27001:2005 «Информационные технологии. Системы информационной безопасности. Требования», можно создать современную СМИБ. Этот стандарт основан на другом известном стандарте - ИСО 9001 «Системы менеджмента качества. Требования», а также по структуре подходит к ИСО 14001 «Системы экологического менеджмента. Требования и руководство по применению». ИСО/МЭК 27001 был разработан на основе пересмотра и адаптации весьма успешного британского стандарта BS 7799, часть 2.

ИСО/МЭК 27001 является документом, в котором сконцентрирована лучшая международная практика, достигнутая в области информационной безопасности. Как это принято в ИСО (международная организация по стандартизации) и МЭК (международный электротехнический комитет), в разработку новых международных стандартов привлекается широкий круг заинтересованных организаций и экспертов посредством технических комитетов [4].

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную систему менеджмента информационной безопасности применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается.

Руководителям организаций следует признать, что информационная безопасность будет результативной и эффективной при условии вовлечения всех структурных подразделений и всех работников в обеспечение информационной безопасности. Этот подход, основанный на общих организационных рисках, отражен в другом стандарте серии ИСО/МЭК 27002:2012 «Информа-

ционные технологии — Методы обеспечения безопасности — Практические правила управления информационной безопасностью» (прежний шифр ИСО/МЭК 17799, переименованный в апреле 2007 года) [15].

Система менеджмента информационной безопасности; СМИБ (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности [8].

Стандартами информационной безопасности называют обязательные или рекомендуемые для исполнения документы, детерминирующие подход к оценке степени безопасности системы.

Стандарты формируют терминологический и понятийный аппарат ИБ, разрабатывают шкалу измерений степени информационной безопасности, повышают технически-информационную совместимость сопутствующей продукции.

Основные сферы стандартизации информационной безопасности: аудит и модели, методы и механизмы обеспечения безопасности, криптография, безопасность межсетевых взаимодействий, управление информационной безопасностью [5].

Обязательным требованием является наличие паспорта на процесс. В таблице 2 представлен разработанный паспорт процесса.

Таблица 2 – Паспорт процесса «Информационная безопасность»

1 Наименование процесса	Информационная безопасность
3 Код процесса	ОП 7.1-01-2017
4 Цель процесса	Отслеживание потока информации и управление передачей данных
5 Владелец	Начальник отдела управления информатизацией
6 Входы	Информация от внешних и внутренних источников (владельцев процесса, подразделений, менеджеров)
7 Поставщики	Внутренние и внешние потребители информации
8 Выходы	Информация с определенным уровнем защиты
9 Потребитель	Подразделения и руководство

Окончание таблицы 2

10 Управляющее воздействие	ГОСТ ИСО 9001-2015; Годовой план производства; СТО 4.3-01-2017, РК, КД, ТД; ИСО/МЭК 27001
11 Ресурсы	Инфраструктура (Оборудование, транспорт) Персонал (Специалисты по информационной безопасности) Производственная среда для функционирования процесса
12 Контролируемые параметры	К – коэффициент защищенности системы информации Sсзи – эффективность системы защиты информации U – ущерб, наносимый системе незащищенной ИБ
13 Критерии результативности процесса	К не более 5% Sсзи≤ΔRи+ΔRои+ΔRсзи, Rсзи≤Sи+Sои
14 Методы измерения	Статистический

Оценочные показатели процесса

Коэффициент защищенности системы информации также можно выразить через риски:

$$K_з = 1 - \frac{R_з}{R_{нз}}$$

где, Rз – риски для защищенной системы,

Rиз – риски для незащищенной системы.

Эффективность систем защиты информации, для которой выполняются следующие условия:

$$\begin{cases} S_{сзи} \le \Delta R_и + \Delta R_{ои} + \Delta R_{сзи}, \\ R_{сзи} \le S_и + S_{ои}, \end{cases}$$

– стоимость защищаемой информации $S_и$;

– стоимость защищаемого объекта информации $S_{ои}$;

– стоимость системы защиты информации $S_{сзи}$;

– суммарный риск информации $R_и$;

– суммарный риск объекта информатизации $R_{ои}$;

– суммарный риск системы защиты информации $R_{сзи}$;

– снижение рисков для информационной системы $\Delta R_и + \Delta R_{ои} + \Delta R_{сзи}$.

На каждом предприятии существует ряд угроз безопасности *(i=0...n)*, которые характеризуются вероятностями возникновения P_{bi}; и ущербом U_i;.

Задачей защиты информации является устранение каждой *i*–й угрозы.

Полный ущерб, наносимый незащищенной системе, определяется:

$$U = \sum_{i=1}^{n} P_{bi} * U_i$$

3.2 Визуализация процесса

Для визуализации разработанного процесса «Информационная безопасность» в ВКР использован метод последовательности блок - схема и метод моделью IDEF0 с помощью программного обеспечения BPWin [16].

С помощью функциональных моделей IDEF, в частности IDEF0, программного обеспечения BPWin дается графическое изображение процесса. Для визуализации в проекте использована функциональная модель IDEF 0. Результат визуализации процесса «Информационная безопасность» представлен в приложении Д. Блок – схема представлена в приложении Е.

Выводы по разделу три

В разделе три разработан процесс «Информационная безопасность» составлен паспорт процесса «Информационная безопасность» для АО «Конар», наглядно представлен процесс с помощью моделей IDEF0 и диаграммы последовательностей (блок-схемы).

4. РАЗРАБОТКА МЕТОДИКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ ПРЕДПРИЯТИЯ»

В данной работе разработана методика информационная безопасность для условий предприятия», которая устанавливает рекомендации по управлению информационной безопасностью предприятия, устанавливает требова-

ния по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ).

Методика состоит из следующих разделов:

1) общие требования;

2) управление системой менеджмента информационной безопасности;

3) функционирование менеджмента информационной безопасности;

4) требования к документации;

5) анализ и оценка риска;

6) обязательства руководства;

7) мониторинг, измерение, анализ и оценка;

8) несоответствия и корректирующие действия.

Разработанная методика «Система менеджмента безопасности для условий предприятия» она прошла апробацию в период март – май на АО «Конар».

5 ОПРЕДЕЛЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ РЕЗУЛЬТАТОВ ВКР

Целью расчета экономического эффекта является выявление величины экономии при реализации результатов выпускного квалификационного проекта.

Для разработки методики системы менеджмента безопасности для условий предприятия, потребовались дополнительные затраты, которые включают следующие статьи:

– затраты на оплату труда;

– затраты на электроэнергию, связанную с технологическими целями (питание компьютера и организационной техники);

– накладные расходы;

– затраты на материалы

Затраты на осуществление методики находятся по формуле (1):

$$Зт = Зт1+Зт2+Зт3+Зт4 \text{ руб.}, \quad (1)$$

где Зт1 – затраты на оплату труда, руб.;

Зт2 – затраты на электроэнергию, руб.;

Зт3 – затраты на накладные расходы, руб.;

Зт4 – затраты на материалы, руб.;

Зт1 находится по формуле (2):

$$Зт1 = Зи+Зс \text{ руб.}, \quad (2)$$

где Зи – заработная плата инженеру по качеству, руб.;

Зс – специалисту по безопасности, руб.;

Находим Зи

Среднемесячная заработная плата инженера по качеству на АО «Конар» составляет 25000, который занимается разработкой методики по 4 часа в день в течение 2 – х месяцев. Оплата часа работы инженера по качеству при восьми часовом рабочем дне пять дней в неделю составляет: $25000/(8 \cdot 5 \cdot 4) = 130,2$

$$Зи = 130,2 \cdot 4 \cdot 2 \cdot 4 + (130,2 \cdot 4 \cdot 2 \cdot 4 \cdot 0,3) = 5416,64 \text{ руб.}$$

Находим Зс

Среднемесячная заработная плата специалиста по безопасности на АО «Конар» составляет 20000, который занимается разработкой методики по 6 часов в день в течение 2 – х месяцев. Оплата часа работы специалиста по безопасности при восьми часовом рабочем дне пять дней в неделю составляет: $20000/(8 \cdot 5 \cdot 6) = 83,33$

$$Зс = 83,33 \cdot 6 \cdot 2 \cdot 4 + (83,33 \cdot 6 \cdot 2 \cdot 4 \cdot 0,3) = 5200 \text{ руб.}$$

В соответствии с формулой (2):

$$Зт1 = 5200 + 5416,64 = 10616, 64$$

Зт2 находится по формуле (3):

$$Зт2 = (N \cdot T \cdot t)/\eta \text{ руб.}, \quad (3)$$

где, N – мощность техники, Т – тариф на электроэнергию, t – время работы техники, η – коэффициент полезного действия.

Мощность техники принимаем 0,5; тариф на электроэнергию 2,04; время работы техники 100; коэффициента полезного действия 0,9.

В соответствии с формулой (3):

$$Зт2 = (0,5 \cdot 2,04 \cdot 100)/0,9 = 113,3 \text{ руб.}$$

Зт3 находится по формуле (4):

$$Зт3 = 0,25 \cdot Зт1 \text{ руб.}, \quad (4)$$

где накладные расходы составляют 25% от затрат на оплату труда.

В соответствии с формулой (4):

$$Зт3 = 0,25 \cdot 10616,64 = 2654,16 \text{ руб.}$$

Зт4 находится по формуле (5):

$$Зт4 = N \cdot Ц \text{ руб.}, \quad (5)$$

где, N – количество.,

Ц – цена, руб.

В соответствии с формулой (5):

$$Зт4 = 5 \cdot 100 + 4 \cdot 10 + 2 \cdot 300 + 4 \cdot 10 + 15 \cdot 15 = 1405 \text{ руб.}$$

Амортизационные отчисления по ВКР находятся по формуле (6):

$$А = Ао + Ап \text{ руб.}, \quad (6)$$

где Ао – амортизационные отчисления оборудования за 2 месяца, руб.,

Ап – амортизационные отчисления программы «Kaspersky Anti – Virus», руб.

Амортизационные отчисления оборудования (принтер, компьютер) находятся по формуле (7):

$$Ао = Цо \cdot 2\% / t \text{ руб.}, \quad (7)$$

где Цо – цена оборудования, руб.;

t – доля года, разработка длилась 2 месяца, отсюда t=12/2=6.

Цк – цена компьютера, равная 30000 руб.,

Цп – цена принтера, равная 8000 руб.

$$Цо=Цк+Цп=30000+8000=38000 \text{ руб.}$$

В соответствии с формулой (6):

$$Ао=38000 \cdot 0,02/6=126,66 \text{ руб.}$$

Амортизационные отчисления программы «Kaspersky Anti – Virus» находятся по формуле (8):

$$Ап=Сп \cdot 20\% / t \text{ руб.}, \quad (8)$$

где, Сп – стоимость программы, руб. Лицензионная программа «Kaspersky Anti – Virus» стоит 2999 рублей в месяц.

t – доля года, разработка длилась 2 месяца, отсюда t=12/2=6.

В соответствии с формулой (8):

$$Ап=5998 \cdot 0,2/6=199,93 \text{ руб.}$$

В соответствии с формулой (6):

$$А=126,66+199,33=326,59 \text{ руб.}$$

В соответствии с формулой (1) получаем:

$$Зт = 10616,64 + 113,3 + 1405 + 2654,16 + 326,59=14789,1 \text{ руб.}$$

В таблице 10 представлена стоимостная оценка всех затрат на внедрение работы.

Таблица 3 – Стоимостная оценка всех затрат на внедрение ВКР

Калькуляция затрат	
Статья	Сумма, руб
Затраты на материалы	1405

Окончание таблицы 3

Затраты на электроэнергию	113,3
Затраты на оплату труда	10616,64
Накладные расходы	2654,16
Амортизационные отчисления	326,59
Затраты на внедрение дополнительных средств защиты	20000
Затраты на обучение	200000
Итого	234789,1

Таблица 4 – Стоимостная оценка всех затрат до внедрения ВКР

Калькуляция затрат	
Статья	Сумма, руб
Затраты на материалы	4 303 753
Затраты на электроэнергию	1 208 000
Накладные расходы	780 023
Затраты на оплату труда	12 345 678
Амортизационные отчисления	477 674
Затраты на внедрение дополнительных средств защиты	899 870
Затраты на программное обеспечение	1 345 821
Итого	9 015 141

В накладные расходы добавляются затраты на разработку ВКР.

Затраты на накладные расходы (Знр2) после внедрения ВКР рассчитываются по формуле (9):

$$Знр2=Знр1–Знр1 \cdot 0,1 \text{ руб.}, \quad (9)$$

где Зм1 – затраты на материалы до внедрения ВКР;

0,1 – процент, на который снижаются затраты на накладные расходы.

$$Зм2=780023–780023 \cdot 0,1=702020,7 \text{ руб.}$$

Внедрение работы повлияет только на уменьшение себестоимости, так как затраты на накладные расходы уменьшатся на 10%, в целом выручка предприятия останется той же. В таблице 12 представлены статьи затрат после внедрения ВКР.

Таблица 5 – Статьи затрат после внедрения ВКР

Калькуляция затрат	
Статья	Сумма, руб
Затраты на материалы	4 303 753
Затраты на электроэнергию	1 208 000
Накладные расходы	702 020,7
Затраты на оплату труда	12 345 678
Амортизационные отчисления	477 674
Затраты на внедрение дополнительных средств защиты	899 870
Затраты на программное обеспечение	1 345 821
Итого	8 937 138

Чистая прибыль до внедрения ВКР (10):

$$ЧП_1 = В_1 – С_1 – Н_1, \text{ тыс.руб.} \quad (10)$$

где $В_1$ – выручка до внедрения ВКР;

$С_1$ – себестоимость до внедрения ВКР;

$Н_1$ – налог на выручку до внедрения ВКР.

Выручка предприятия до внедрения ВКР считается по формуле (11):

$$В = N \cdot К, \text{ тыс.руб.} \quad (11)$$

Где N – количество выпускаемой продукции;

К – цена одного изделия;

В соответствие с формулой (11) получим:

$$В_1 = 238800 \cdot 100 = 23880000 \text{ тыс.руб}$$

Налог на выручку считается по формуле (12):

$$Н = (В – С) \cdot 0,2, \text{ тыс.руб} \quad (12)$$

$$Н_1 = (23880000 – 9015141) \cdot 0,2 = 2972971,8, \text{ тыс.руб.}$$

В соответствие с формулой (10) получаем:

$$ЧП_1 = 23880000 – 9015141 – 2972971,8 = 11891888 \text{ тыс.руб}$$

Чистая прибыль после внедрения ВКР (13):

$$ЧП_2 = В_2 – С_2 – Н_2, \text{ тыс.руб.} \quad (13)$$

где $В_2$ – выручка до внедрения ВКР;

C_2 – себестоимость до внедрения ВКР;

H_2 – налог на выручку псоле внедрения ВКР.

Выручка предприятия до внедрения ВКР считается по формуле (14):

$$B_2 = N_2 \cdot K_2, \text{ тыс.руб.} \quad (14)$$

Где N – количество выпускаемой продукции;

K – цена одного изделия;

В соответствие с формулой (12) получим:

$$B_2 = 238900 \cdot 100 = 23890000 \text{ тыс.руб}$$

Налог на выручку считается по формуле (13):

$$H_2 = (23890000 – 8937138) \cdot 0{,}2 = 2990572, \text{ тыс.руб}$$

В соответствие с формулой (16) получаем:

$$ЧП_2 = 23890000 – 8937138 – 2990572 = 11962289, \text{ тыс.руб.}$$

Ожидаемый экономический эффект считается по формуле:

$$Эож = ЧП2 – ЧП1, \text{ тыс.руб} \quad (15)$$

В соответствие с формулой (20) получим:

$$Эож = 11962289 – 11891888 = 70401 \text{ тыс.руб.}$$

Ожидаемый экономический эффект от результатов работы находим по формуле (16):

$$Эож_т = Эож_i/(1+r)^2 \quad (16)$$

где r – норма дисконта;

T – расчетный период.

Период – 6 лет, норма дисконта 0,19.

В соответствие с формулой получаем:

$Эож^6 = 70401/(1+0{,}19) + 70401/(1+0{,}19)^2 + 70401/(1+0{,}19)^3 + 70401/(1+0{,}19)^4 + 70401/(1+0{,}19)^5 + 70401/(1+0{,}19)^6 = 59160 + 29580 + 19720 + 14790 + 11832 + 9860 = 144942$ тыс.руб

Ожидаемый экономический эффект с учетом дисконтирования за каждый год расчетного периода представлен в таблице 14.

Таблица 6 – Ожидаемый экономический эффект с учетом дисконтирования за каждый год расчетного периода

Расчетный период	Прибыль с учетом дисконта
2017	59160
2016	29580
2015	19720
2014	14790
2013	11832
2012	9860

Ниже представлена диаграмма ожидаемого экономического эффекта.

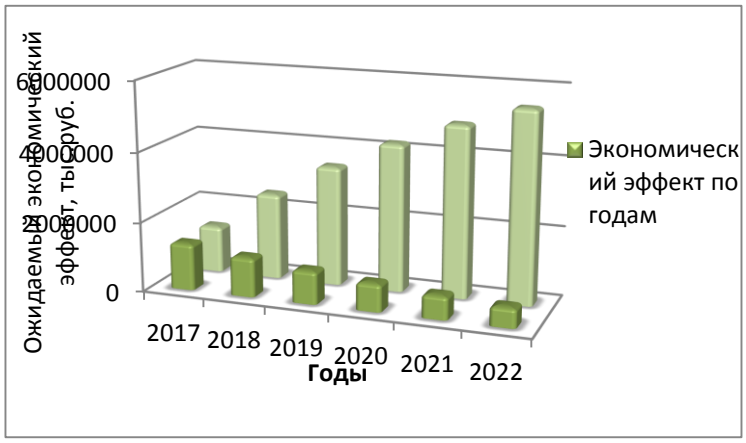


Рисунок 6 – Диаграмма ожидаемого экономического эффекта с учетом дисконтирования за каждый год расчетного периода

Выводы по разделу шесть

Годовой экономический эффект составил 70401 тыс.руб, он получен за счёт сокращения затрат на накладные расходы (10%). А суммарный экономический эффект составил 144942.

ЗАКЛЮЧЕНИЕ

В ходе выпускной квалификационной работы была достигнута цель предприятия, а также выполнены следующие задачи: проведен анализ состояния дел на предприятии в ходе которого были рассмотрена история предприятия, его цели, а также были выявлены проблемы предприятия в области информационной безопасности, проведено сравнение передовых отечественных и зарубежных методов информационной безопасности, выбраны наиболее эффективные методы, которые не требуют больших материальных затрат, усовершенствован процесс «Информационная безопасность», приведен его паспорт, а также графическое описание методами «Блок-схема процесса» и «IDEF0 – моделирование», разработана методика информационная безопасность для условий предприятия, определен ожидаемый экономический эффект от внедрения результатов ВКР.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Коротченко, С.Е. Развитие информационной безопасности России на современном этапе/ С.Е. Коротченко – Кубанский государственный университет, 2016 – 10 с.

2 Белов, Е.Б. Основы информационной безопасности./ В.П. Лось., Е.Б. Белов – М. : Горячая линия : Телеком, 2006. – 544 с.

3 ГОСТ Р 50922-96 Защита информации. Госстандарт России, Требования.– М.: ИПК Издательство стандартов, 2015. – 32 с

4 Нестеров, В.И Основы информационной безопасности./ В.И. Нестеров – Учебное пособие. М.: Издательский центр «Сатурн», 2014. – 368 с

5 Ерохин, В.В., Безопасность информационных систем. / В.В. Ерохин, И.Г. Степченко – Учебное пособие. Гриф МО РФ. М.: Издательский центр «Телеком», 2010. – 467 с.

6 РК-2014. Система менеджмента качества. Руководство по качеству. – Челябинск: АО «Конар», 2014. – 69 с.

7 ГОСТ ISO 9001 – 2015. Система менеджмента качества. Требования.– М.: ИПК Издательство стандартов, 2015. – 32 с.

8 ГОСТ Р ISO/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.– М.: ИПК Издательство стандартов, 2006. – 27 с.

9 Алферов, А.П. Основы криптографии. / А.П. Алферов, А.П., Зубов, А.Ю., Кузьмин, А.С., Черемушкин, А.В. – М.: Юрлитинформ, 2012. – 296 с.

10 Аверченков, В.И. Аудит информационной безопасности, учебное пособие для вузов./ В.И. Аверченков — 2-е изд., стереотип. — М.: ФЛИНТА, 2011. — 269 с. — ISBN 978-5-9765-1256-6.

11 Лапонина, О.В. Основы сетевой безопасности / О.В. Лапонина – М.: Профинформ, 2009. – 296 с.

12 Schinier, B. Applied Cryptography,/ B. Schinier – John Wiley & Sons, 1996 – 784p.

13Cheswick, W.R. Firewalls and Internet Security: Repelling the Wily Hacker. / W.R. Cheswick, S.M. Bellovin, S.M - Addison-Wesley, 2008. – 324 p

14Статьев, В.Ю. Информационная безопасность распределенных информационных систем. Информационное общество/ В.Ю Статьев, В.А. Тиньков. – 1 выпуск, 2008 – 71с.

15 ИСО/МЭК 27002:2012 «Информационные технологии — Методы обеспечения безопасности — Практические правила управления информационной безопасностью», 2012 – 45 с.

16 Маклаков, С.В. Моделирование бизнес-процессов с All-Fussion Process Modeler (BPWin 4.1)/ С.В. Маклаков. – М.: ДИАЛОГ-МИФИ, 2003 – 240 с

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

18Беляев, В.К. Экономическая оценка управленческих решений/ В.К Беляев. – Нюренберг. Baikal Research Journal. 2015. Т. 6. № 4. С. 16

19Гречкина, О.В. Всеобщее управление качеством / О.В. Гречкина – М.: Юрлитинформ, 2010. – 296 с.

20Вишняков И.А. Общая теория рисков. / И.А. Вишняков, В.Р. Радаев – 2-е изд., перераб. и доп. — М.: Издательская корпорация «Логос», 2008. — 200 с.

21 Василенко, И.А. Методы и модели классифицирования рисков. / И.А. Василенко. – 1-е изд., перераб. и доп. — М.: Издательская корпорация «Логос», 2010. — 100 с. [Электронный ресурс] – http://finlit.online/ekonomika-otrasli/tselesoobraznost-ispolzovaniya-nechetko-8110.html.

ПРИЛОЖЕНИЕ А

Модель процесса «Информационная безопасность»

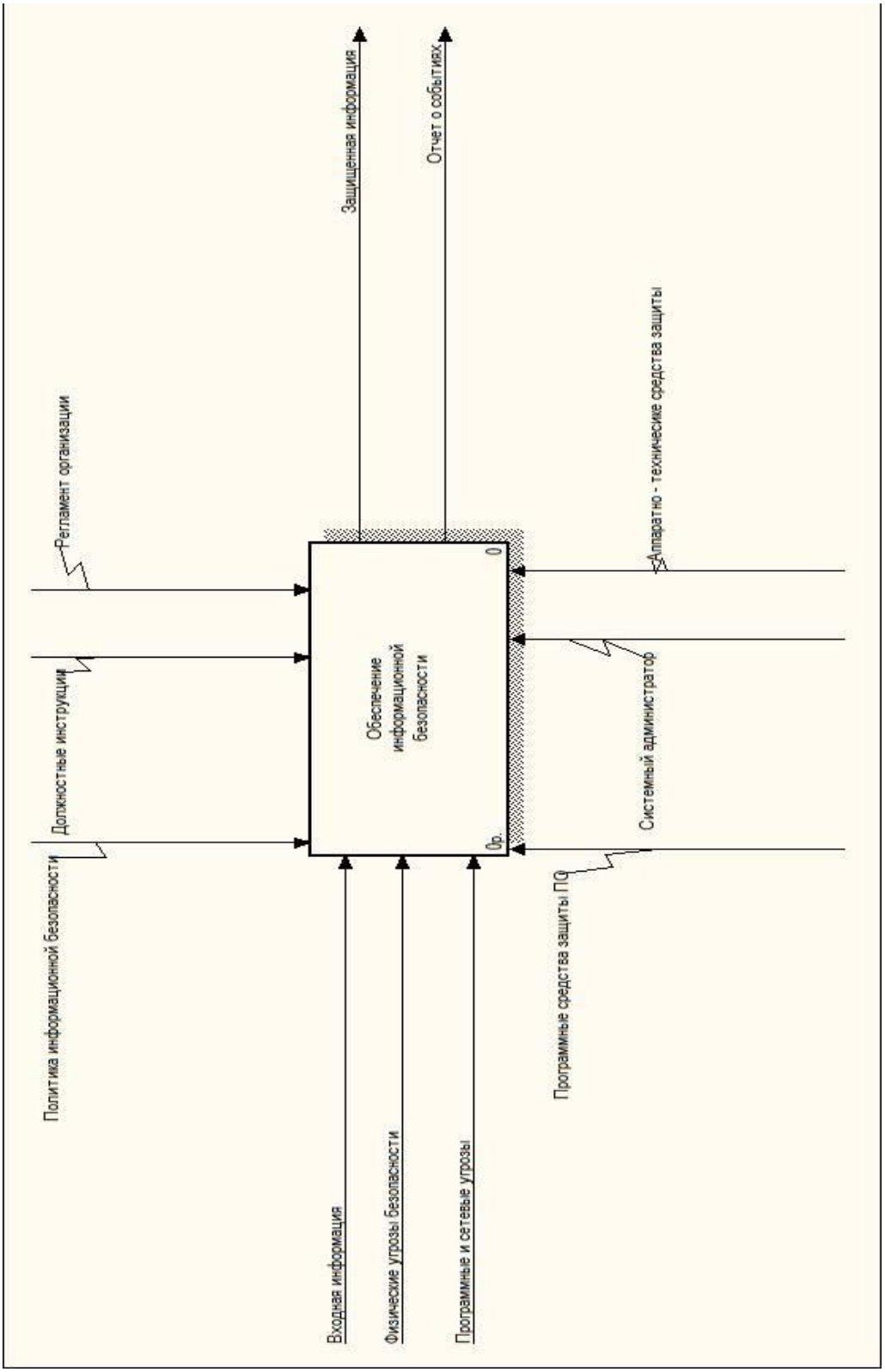


Рисунок А.1 – Модель процесса « Информационная безопасность

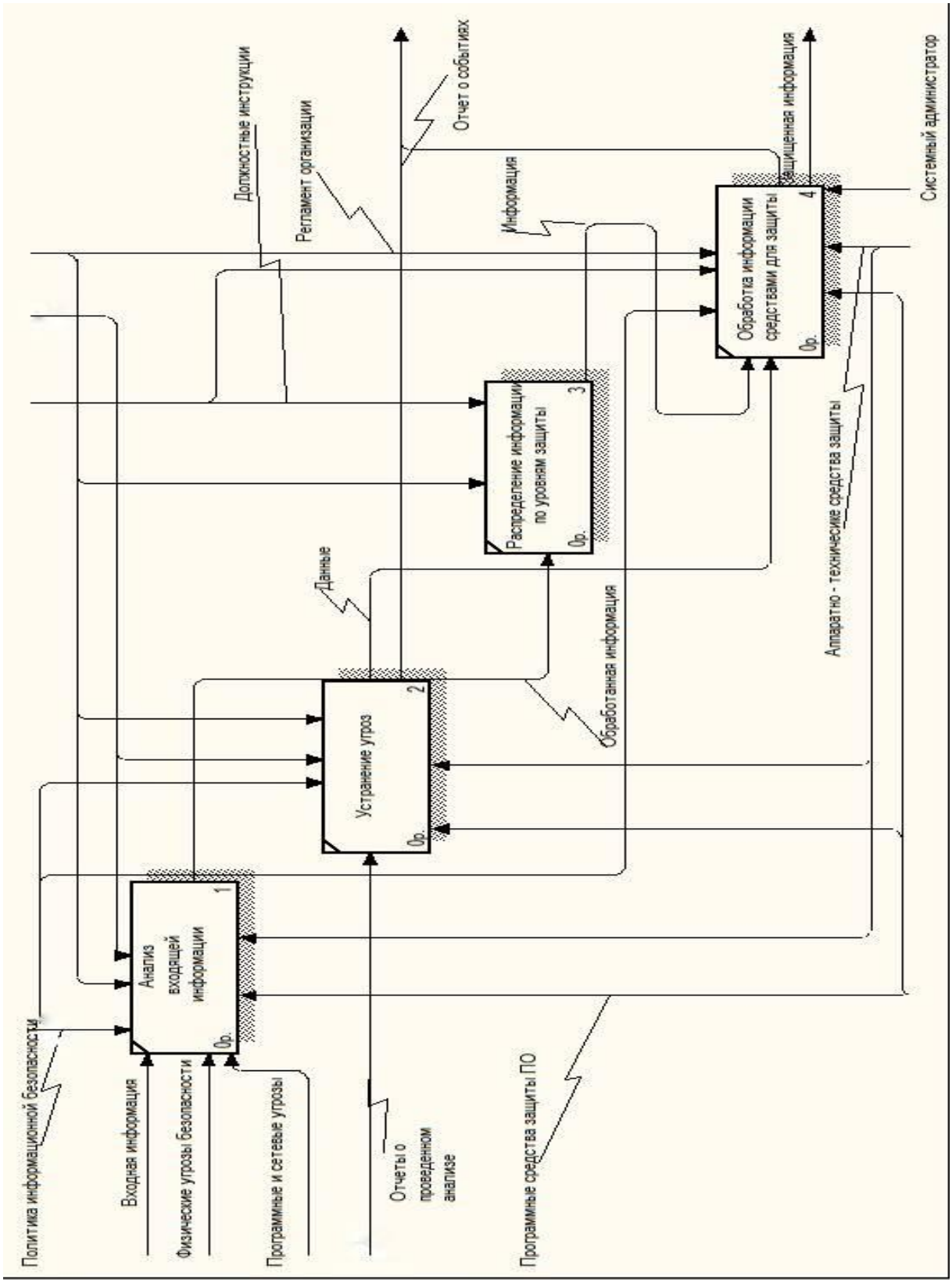
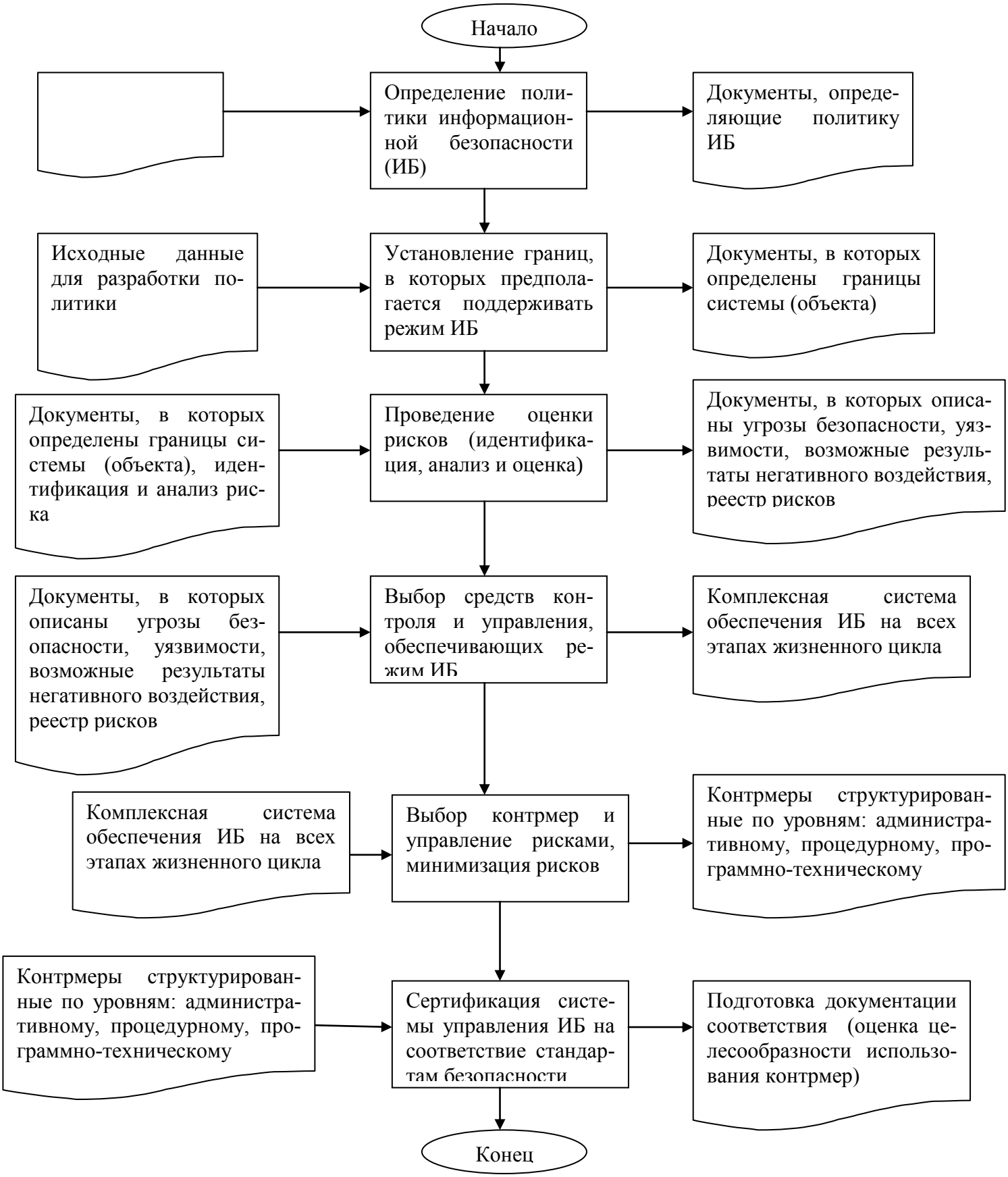


Рисунок А.2 – Модель процесса «Информационная безопасность

ПРИЛОЖЕНИЕ Б

Блок – схема процесса «Информационная безопасность»



ПРИЛОЖЕНИЕ В

Анализ галстук-бабочка для процесса «Информационная безопасность»

Рисунок В.1 – Анализ «галстук – бабочка»