МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра Систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Комплексная система защиты информации производственного предприятия
Специальность 5В100200 – «Системы информационной безопасности»
Выполнил Тохта-Муратов Бекет Сергалиевич Группа СИБ-15-2
Научный руководитель Покусов Виктор Владимирович

Консультант:
по экономической части:
к.э.н., профессор Аренбаева Ж. Г.
(ученая степень, звание, Ф.И.О)
_____ «27» мая 2019 г.
(подпись)

по безопасности жизнедеятельности:
д.т.н. ст. преп. Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О)
_____ «28» мая 2019 г.
(подпись)

по применению вычислительной техники:
ст. преп. Покусов В.В
(ученая степень, звание, Ф.И.О)
_____ «28» мая 2019 г.
(подпись)

Нормоконтролер:
ст. преподаватель Исмагулова Н.Т
(ученая степень, звание, Ф.И.О)
_____ «5» июня 2019 г.
(подпись)

Рецензент:
_____
(ученая степень, звание, Ф.И.О)
_____ «_____» _____2019 г.
(подпись)

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра систем информационной безопасности

Специальность 5В100200 – «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Тохта-Муратову Бекету Сергалиевичу

Тема проекта Комплексная система защиты информации производственного предприятия

Утверждена приказом по университету №_184_ от «_26_» _октября_2018 г.

Срок сдачи законченного проекта «_____» _____2019 г.

Целью дипломной работы является внедрение комплексной системы защиты информации производственного предприятия.

Для достижения указанной цели необходимо решить следующий комплекс задач:

- изучить общую структуру производственного предприятия;
- определить потенциальные источники угроз и уязвимые места;
- изучить и сравнительно проанализировать современные методы и системы защиты информации;
- внедрить оптимальный метод защиты информации для предприятия.

Перечень вопросов, подлежащих внедрению в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект включает в себя 5 глав, разделенных на подглавы, каждая из которых освещает определенную тематику, используемую при внедрении систему защиты информации.

В первой главе дипломного проекта представлена общая информация при исследовании и приемлемого метода технической защиты.

Во второй главе дипломного проекта представлена внедрение аппаратно-программного решения и разработка рекомендации по снижению рисков в информационной системе предприятия.

В третей главе подробно описывается оценка рисков информационной безопасности предприятия.

В четвертой главе рассматриваются необходимые условия для комфортной работы сотрудников предприятия.

В пятой главе проводится технико-экономическое обоснование.

Основная рекомендуемая литература:

1 Березюк, Л.П. Организационное обеспечение информационной безопасности : учеб. пособие / Л.П. Березюк. – Хабаровск: Изд-во ДВГУПС, 2008. – 188 с.

2 Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам – Учебное пособие – М.: Горячая линия - Телеком, 2011. – с. 220.

3 Корниенко А.А., Слюсаренко И.М. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования ПГУПС, «InfoSoftCom» 2009 г.

4 КубеевЕ.К., Каргин С.Т. Учебный процесс в КарГУ. - Караганда: Изд-во КарГУ, 2003. – 9 с.

5 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

6 Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. – М.: Гелиос АРВ, 2005 г. – 224 с.

7 Баранова Е.К. Методики анализа и оценки рисков информационной безопасности. Статья. УДК 519.876.5 2015 г.

8 Будников А.И. Информационная безопасность и защита информации. 2014 год. Статья. ИНФ 217.671.8 2016 г.

Конструкции по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Эконом. часть	Аленбаева Ж.Г.	04.03-27.05	
Безоп. жизн.	Бекбосаров Ш.Ш.	04.03-28.05	
Выпуск. техника.	Понусов В.В.	18.05-28.05	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Исследование и выбор метода ТЗ	01.02.2019 - 15.02.2019	
Тех. характеристика системы	15.02.2019 - 01.03.2019	
Внедрение АРК „Инспектор"	01.03.2019 - 12.03.2019	
Реализация системы мониторинг	12.03.2019 - 30.03.2019	
Анализ результатов внедрения	30.03.2019 - 12.04.2019	
Разработка мик. рисков	12.04.2019 - 25.04.2019	
Оценка рисков ИБ	25.04.2019 - 01.05.2019	
Аппаратно-прог. комплекс „Инсп"	01.05.2019 - 15.05.2019	

Дата выдачи задания «___» _____ 2019 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Покусов В.В.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студента Текем (Толта-Мурат Ф.С)
(Подпись) (Ф.И.О)

АҢДАТПА

Осы дипломдық жұмыста өндірістік кәсіпорынның кешенді ақпараттық қауіпсіздік жүйесі талданды. Зерттеу кезінде үздік әрі экономикалық тиімді шешімдер табылды.

Талдау нәтижелері бойынша «Инспектор» бағдарламалық-техникалық кешені таңдалды. Сондай-ақ, осы өнімді таңдау үшін барлық функциялар мен негіздемелер беріледі.

Нәтижесінде кәсіпорында «Инспектор» бағдарламалық-аппараттық кешен орнатылды. Бұл «PC4U» өндірістік кәсіпорнында байланыс арналары арқылы шектеулі қолжетімділіктің ақпараттарының ағып кетуін болдырмау мәселесін шешуге мүмкіндік берді.

АННОТАЦИЯ

В данной дипломной работе проведен анализ комплексной системы защиты информации на производственном предприятии. В ходе исследования были определены наиболее оптимальные и экономические доступные технологические решения.

По результатам анализа был выбран программно-аппаратный комплекс «Инспектор». Так же приведены все функционалы и обоснование причин для выбора данного продукта.

В результате был установлен на предприятии программно-аппаратный комплекс "Инспектор". И позволило решить задачу блокирования утечки информации ограниченного доступа через каналы связи на производственном предприятии ТОО «PC4U».

ANNOTATION

In this thesis, an analysis of the integrated information security system at a manufacturing enterprise. During the study, the most optimal and economically accessible technological solutions were identified.

According to the results of the analysis, the «Inspector» software and hardware complex was selected. All functionals and rationale for the selection of this product are also given.

As a result, the Inspector software and hardware complex was installed at the enterprise. And it allowed to solve the problem of blocking information leakage of limited access through communication channels at the production enterprise «PC4U» LLC.

Содержание

Введение

Актуальность темы. Стремительное развитие информационных технологий в производственном секторе привело к увеличению числа проблем информационной безопасности (ИБ) в производственном секторе. В настоящее время наблюдается снижение уровня безопасности системы в связи с повышением открытости информационной системы (ИС) и интенсивности обмена информацией с пользователями и внешними ресурсами. Это может привести к большим финансовым потерям для компании в будущем. В этой связи как для компании-производителя, так и для любого коммерческого предприятия важно провести тщательный анализ защиты интеллектуальной собственности и рисков, чтобы оценить степень потенциальных потерь и определить оптимальный способ защиты информации[1].

Производственные объекты представляют собой инфраструктуры с множеством разнообразных данных и информации, которые нуждаются в защите[2]. Рост числа атак на информационную систему требует защиты информационных ресурсов и создает проблему построения собственной комплексной системы безопасности. Его решение предполагает наличие единой правовой базы, создание концепции безопасности, проведение организационных работ и применение технических средств защиты информации (ТСЗ) в рамках промышленной компании. Представленные основные компоненты определяют единое руководство по обеспечению информационной безопасности в компании[3].

Качественное создание защищенной информационной системы заключается в выборе оптимального способа защиты информации, отвечающего всем параметрам критерия эффективности и учитывающего наличие слабых мест и их взаимодействие. В этом контексте одной из самых актуальных проблем, с которой сегодня сталкиваются разработчики Информационных систем (ИС) и сотрудники службы технической поддержки, является полное решение проблемы ИС с момента создания концепции, политика компании в области ИС до разработки определенных методов и рекомендаций по ее сопровождению.

Объектами системы защиты информации[4] являются: сервер базы данных, защита интеллектуальной собственности, консоль управления счетами, сервер и ЛВС, учетная ЛВС, данные планово-финансовой службы, статистические и архивные данные.

Данная работа посвящена систематической презентации политики, стандартов, технологий и процедур информационной безопасности информационных систем компании, а также описанию высокоэффективных методов, предлагаемых для предоставления ИС на основе внедрения технологии DataLeakPrevention (DLP).

Научной новизной. является разработка оптимального метода защиты информации в компании, учитывающего наличие уязвимостей и различных угроз, а также концепции СИ компании.

Полученные результаты:

В работе проводится анализ и теоретическое обобщение известных методов защиты от угроз конфиденциальной информации применительно к данной компании, разрабатываются практические рекомендации по снижению уязвимости системы обеспечения безопасности СИ. Основные результаты работы:

1) вы получите ряд угроз безопасности и уничтожение целостности информации компании, предоставляющей ограниченный доступ;

2) классификация специфических наборов методов и инструментов защиты от различных видов угроз (несанкционированного доступа, шпионажа и физического воздействия, компьютерных вирусов, взлома корпоративных систем);

3) разработка алгоритмов анализа и оценки уязвимости автоматизированных систем компании;

4) разработана концепция СИ производственной компании ТОО «PC4U»;

5) рекомендации по снижению уязвимости разрабатываемой системы информационной безопасности;

6) полученные теоретические и прикладные материалы проходят испытания в информационной системе ТОО «PC4U».

Теоретическая значимость заключается в научной логике современного подхода и содержании выводов, предложений и рекомендаций, обобщающих и дополняющих научные знания в области информационной безопасности.

Анализ потенциальных угроз и предлагаемых систем защиты от них углубляет и расширяет общее содержание теории защиты информации по отношению к университету. Полученные результаты систематизируют информацию теории защиты информации для компании с учетом особенностей ее функционирования.

Практическая значимость.

Методы, предлагаемые для предоставления ИС локальным серверам операционных систем, будут протестированы и предложены для внедрения и использования в компании-производителе.

Цель и задачи дипломной работы. Целью работы является разработка оптимального способа защиты информации в производстве.

Для достижения этой цели необходимо решить следующий комплекс задач:

1) сбор информации по теме дипломной работы;

2) исследование общей структуры информационной системы компании;

3) выявление потенциальных источников угроз и уязвимостей;

4) исследование и сравнительный анализ современных методов и систем защиты информации;

5) разработка оптимального метода защиты информации для добывающей компании.

Предметом дипломного исследования является производственное предприятия.

Тема исследования – комплексное система защиты информации на производственном предприятии.

Обзор существующих методов и средств обеспечения безопасности информационных систем, анализ построения информации о компании-производителе, выбор оптимального способа защиты информационного общества.

Надежность результатов работы.

Достоверность позиций и выводов по результатам работы определяется результатами, полученными в ходе расследования в работе.

Теоретической основой работы являются такие научно-исследовательские работы, как компьютеризация работы и системы управления на предприятии, анализ методов и средств защиты информации, информационной безопасности и защиты информации на предприятии, анализ источников опасности, атак на сети и их влияния, которые рассматриваются отечественными и зарубежными учеными и изучаются:А.И. Будников, В.Ф. Шаньгин, С.Д. Рябко, А.В. Галицкий, В.В. Поляков, А.В. Головин, В.А. Мазуров, С.И. Макаренко, М.И. Шубинский, М. Лунгу, И.М. Ажмухамедов, О.М. Проталинский [3, 10,20, 24, 26, 34, 37].

Методологической основой работы являются такие направления исследований, как анализ систем информационной безопасности, которые описаны в работе следующих ученых:М.И. Шубинский, М.Лунгу, И.М. Ажмухамедов, О.М. Проталинский, В.Л. Усков, А.Д. Иванников, А.В. Усков [2, 3, 10, 20].

Практической основой для создания работы является комплексная система информационной безопасности на производственном предприятии.

Структура и объем работы. Работа состоит из введения, основной части, заключения, списка использованной литературы. Объем введения - 5 страниц, основная часть - 56 страниц, выводы - 3 страницы. дипломная работа содержит 22 рисунков и 11 таблиц. Список библиографических источников включает 30 наименований.

Введение содержит обоснование актуальности темы дипломной работы, научной новизны и практического значения, оценку текущего состояния решаемой дипломной задачи. Приводятся цель, задачи, тема дипломной работы, теоретические и методические основы и практические основы дипломной работы. Введение состоит из 5 страниц.

Основная часть документа содержит данные, отражающие характер, содержание, методологию и основные результаты дипломной работы. Основная часть состоит из трех глав и 56 страниц.

Первая глава содержит анализ и обоснование оптимального метода технической защиты, обосновывающее внедрение нового метода защиты в СВК, технические требования системы "Инспектор", описание аппаратно-программного комплекса (АПК) системы "Инспектор".

Вторая глава посвящена внедрению и внедрению системы мониторинга "Инспектор" в СИ ТОО «PC4U», анализу результатов внедрения системы и рекомендациям по снижению рисков в информационной системе компании. Третья глава состоит из 18 страниц.

Третья глава содержит оценку рисков информационной безопасности на предприятии с помощью АПК "Инспектора" (DLP - System) в ТОО "PC4U".

Четвертая глава описывает систему искусственного освещения и вентиляцию воздуха для нормальной работы сотрудников.

Пятая глава содержит экономические расходы, которые нужны для проектирование программно-аппаратного комплекса. Расходы состоят из: себестоимость, прибыль и цена с учетом НДС.

Трехстороннее заключение содержит краткие выводы по результатам исследования, содержащие оценку целостности задач, конкретные предложения и рекомендации по защите ТОО "ИГ ТОО "ПК4У".

Перечень используемой литературы представляет собой перечень используемых научных статей, учебников, электронных источников и содержит 30 наименований.

Ключевые слова по теме работы: информационная система, информационная безопасность, межсетевой экран, VPN, система "инспектор", сетевые атаки, источники опасности, защита информации от утечек, DLP система, требования к защите информации, мониторинг, консоль администратора, база данных, эффективность защиты информации, оптимальный способ защиты.

1 Исследование и выбор приемлемого метода технической защиты

1.1 Внедрения оптимальной реализации метода защиты информации на производственном предприятии

В соответствии с Законом Республики Казахстан "Об информатизации", Законом Республики Казахстан "О персональных данных и их защите", необходимо принять меры по защите персональных данных от раскрытия, использовать меры по защите электронных информационных ресурсов и использовать системы контроля доступа и записи доступа к информации.

Защита персональных данных – совокупность технических, организационных, теоретических и правовых мер по защите информации конкретного лица – субъекта персональных данных (сотрудников)[28].

В соответствии с Законом Республики Казахстан "О персональных данных и их защите", сбор, обработка и защита персональных данных осуществляется в соответствии с принципами[28]:

1) конфиденциальность персональных данных с ограниченным доступом;

2) гарантировать безопасность личности, общества и государства.

3) законность;

4) уважать права человека и гражданина, конституционные свободы;

5) равные права субъектов, владельцев и операторов;

В соответствии с постановлением правительства №832 от 20 декабря 2016 года о принятии единообразных требований к информационно-коммуникационным технологиям и гарантии информационной безопасности компании обязаны контролировать действия пользователей и сотрудников, контролировать использование средств обработки информации и регистрировать события и события, а также другие меры контроля и защиты информации.

Постановление правительства №832 от 20 декабря 2016 года требует регистрации инцидентов в области информационной безопасности:

- автоматическое создание записей администратора;
- внедрение систем мониторинга инцидентов и проявлений и событий ИБ;
- уведомления, основанные на автоматическом обнаружении подозрительного события или инцидента ИБ.

На этапе опытно-промышленной эксплуатации объектов, средств и систем компьютеризации должны использоваться [29]:

- предотвращения и выявление вредоносного кода;
- управления событиями и инцидентами ИБ;
- предотвращения и обнаружения вторжений;
- управления и мониторинга информационной инфраструктурой.

Согласно СТ РК 1699-2007, системы контроля и управления доступом должны соответствовать всем необходимым требованиям и обеспечивать [30]:

- запись и регистрация подозрительных и текущих сообщений;

- демонстрация подозрительных событий;

- защита программного и аппаратного обеспечения от несанкционированного доступа;

- автоматический контроль удобства использования инструментов и информационных линий, содержащихся в системе;

- возможность автономной органов управления системы;

- точки доступа могут быть заблокированы командой с контрольной точки в случае атаки;

- возможность подключения вспомогательных средств специального контроля, средств досмотра.

Основными методами технической защиты являются информационные системы ТОО "PC4U":

1) обеспечения целостности;

2) защита и управление информационной компьютерной сетью;

3) контроль доступа;

4) регистрация и отслеживание действий ПК;

5) антивирусная защита;

Проведя анализ информационной безопасности организации ТОО "PC4U", исследование информационных ресурсов, было установлено, что контроль доступа осуществляется службой каталогов ActiveDirectory, антивирусная защита обеспечивается антивирусным ПО "Антивирус Касперского", базовая защита информационной компьютерной сети обеспечивается системой KerioWinroute.

Технология ActiveDirectory - это служба каталогов, разработанная Microsoft. Справочная служба предназначена для хранения информации обо всех сетевых ресурсах, содержит данные в организованном формате и обеспечивает оптимизированный доступ к ним. Клиенты могут отправлять определенные запросы ActiveDirectory для получения информации о каждом сетевом объекте.

Список функций ActiveDirectory включает следующие основные функции[31]:

- безопасное хранение данных. Каждый объект ActiveDirectory имеет свой собственный список контроля доступа (ACL);

- многофункциональный механизм поиска, основанный на Глобальном каталоге (ГК), созданном AD. Все сотрудники, работающие в DA, могут получить доступ к этой директории.

Синхронизация данных упрощает доступ к информационным ресурсам и повышает доступность и надежность всего сервиса.

Комплексная концепция расширения, позволяющая расширить существующие объекты новыми типами.

Сетевое взаимодействие по нескольким протоколам. Служба ActiveDirectory основана на модели X.500 и поддерживает сетевые протоколы, такие как LDAP 2, LDAP 3 и HTTP.Служба DomainNameSystem (DNS)[31]

используется для реализации службы DomainNameControllerService и поиска сетевых адресов.

Для реализации службы имен контроллеров доменов и поиска сетевых адресов используется служба DNS (DomainNameSystem – система доменных имен) [31].

Антивирус Касперского - это продукт, предназначенный для защиты ПК от вредоносных программ, троянов, шпионских программ и неизвестных угроз посредством защиты в режиме реального времени, включая HIPS. Общий комплекс программы включает в себя: антивирусные файлы, почту и интернет.

Антивирус Касперского состоит из:

1) компоненты защиты, защищающие ПК на всех каналах приема и передачи информации;

2) задачи антивирусного сканирования, которые сканируют ПК или отдельные файлы, каталоги, жесткие диски, документы для обнаружения вирусов;

3) сервисные опции, обеспечивающие информационную поддержку при работе с программой и позволяющие расширить ее функциональность;

4) предоставляет пользователю защиту от вирусов;

5) функции Антивируса Касперского;

6) безопасность рабочих станций, где осуществляется многоуровневая защита, обновление систем безопасности, защита от угроз, предотвращение и блокировка сетевых атак, интеграция с облачными средами;

7) безопасность файлового сервера;

8) обеспечивает централизованное управление.

Компьютерный вирус - это вредоносная программа, которая воспроизводит себя и может также встраиваться в другие программы, системную память, загрузочные файлы и сектора. Вирусы запрограммированы на прерывание работы программ, блокирование работы пользователей, уничтожение файлов и документов, деактивацию аппаратных комплексов ПК.

Основные источники вирусов[28]:

1) содержатся в дискетах, файлах и документах;

2) компьютерная сеть, включая систему электронной почты и интернет;

3) жёсткий диск;

4) оставшийся в оперативной памяти вирус.

Брандмауэр KerioWinroute - это программный пакет для доступа в Интернет по локальной сети компании. Этот продукт отличается гибкой и быстрой конфигурацией, интеграцией в существующую сеть компании с поддержкой ActiveDirectory и других программ Microsoft, высоким уровнем безопасности системы, поддержкой построения корпоративной виртуальной сети через Интернет, простотой администрирования и требованиями к ресурсам[23].

Программа KerioWinRouteFirewall определяет правила доступа для детального анализа всего Интернет-трафика, проходящего и адаптируемого к политике IP безопасности, обеспечивая высокий уровень безопасности для всей информационной системы и удаленных компьютеров, работающих через Интернет.

С помощью этого продукта установка виртуальной частной сети практически так же проста, как и может быть. VPN сервер и VPN клиенты являются частью безопасного удаленного доступа WinRouteFirewall к корпоративной сети. Использование виртуальной сети Kerio VPN позволяет пользователям удаленно подключаться ко всем ресурсам образовательной сети [http://compress.ru/article.aspx?id=20549].

Встроенный в KerioWinRouteFirewall VPN сервер позволяет организовать VPN сети в двух различных сценариях: Сервер и клиентский сервер (Kerio VPN клиент используется для Windows, Mac и Linux).

Продукт KerioWinRouteFirewall имеет следующие особенности:

1 Брандмауэр защита от вирусов:

- электронная почта (SMTP и POP3);
- пересылка файлов (FTP);
- WEB (HTTP).

2 Сканирование и фильтрация:

- HTTP-фильтр для всплывающих окон;
- FTP-фильтр и верификация.

3 Управление пользователями. KerioWinRouteFirewall позволяет администраторам устанавливать и применять ограничения для каждого пользователя, в дополнение к анализу использования трафика. Например, поддержка ActiveDirectory.

4 Поддержка UPnP. Этот продукт позволяет работать вместе без дополнительных настроек для различных областей применения.

5 Дистанционное администрирование. Если администратор не может контролировать все процессы в системе брандмауэра, то можно сообщить администратору о событиях ИС: статистику о предпочтениях преподавателей, учащихся и других пользователей, использование трафика по типу, посещения WEB-страниц, перегрузку трафика, различные проблемы. Программа сохраняет все изменения и дает результаты.

Метод защиты информационной системы, используемый в организации ТОО "PC4U", недостаточен для управления персональным компьютером, невозможно расследовать инциденты с важными персональными и деловыми данными, конфиденциальными информационными ресурсами.

Основными недостатками ИБ ТОО "PC4U" являются отсутствие полного контроля над последующими действиями сотрудников:

- обработка информации (в общей папке);

- пересылка по электронной почте;
- пересылка на печать;
- копирование информации;
- посещение web-сайтов.

Таблица 1 - Статистический анализ угроз, обнаруженных в ТОО "PC4U"

Наименование	2016	2017	2018
Компьютерные вирусы	1700	2300	
Умышленное неправомерное использование и/или недобровольные ошибки со стороны сотрудников	0	0	
Несанкционированный доступ к информации	0	0	
Отсутствие технического обслуживания системы	3	1	
Проникновение в информационную систему	0	0	
Умышленное неправомерное использование и/или непреднамеренные ошибки сотрудников при работе в беспроводных сетях.	2	2	
Кража конфиденциальной частной информации	0	0	
Ошибки при работе с открытыми веб-приложениями	2	4	
Сетевые атаки на веб-сайты	0	0	

В результате проведенного анализа я пришел к выводу, что в целях повышения информационной безопасности с технической точки зрения и выполнения требований законодательства Республики Казахстан необходимо внедрить систему мониторинга и контроля информации на персональных компьютерах.

Система мониторинга является одним из ключевых компонентов информационной безопасности, так как для каждой компании важно знать информацию обо всех сделках и действиях, к которым она ведет. Эти системы представляют собой сложное программное или аппаратное и программное обеспечение, которое может отслеживать деятельность пользователей, предотвращать утечку конфиденциальной информации и выявлять ненадлежащее использование рабочего времени. Отслеживая все действия сотрудников на ПК, вы можете улучшить качество своей работы и повысить ее эффективность.

Высокие стандарты качества и нормативные требования большинства крупных предприятий Казахстана требуют интегрированной системы управления для обеспечения надежного хранения данных. Необходимость создания таких систем обусловлена ростом внутренних угроз.

Система мониторинга и контроля информации на ПК включает в себя технологию предотвращения утечки данных (DLP).

Системы DLP - это аппаратные и программные технологии, которые могут предотвратить случайную или преднамеренную потерю конфиденциальной информации. Эти технологии работают совместно в комплексе с различными системами, используемыми для защиты информационной системы[29].

Набор функций, которые помогают обнаружить и заблокировать передачу информации из корпоративной системы в сеть:

Набор функций, позволяющих обнаружить и заблокировать передачу информации из системы предприятия в сеть: фильтрация интернет-трафика и информационных потоков;

Проводить анализ содержания на основе предопределенных ключевых слов, "оцифрованных" документов и конкретных выражений.

Системы DLP обеспечивают три уровня защиты от потери конфиденциальной информации:

1 Перемещение данных - Защита информации во время передачи данных по информационным каналам. Это делается в этом процессе:

- оценка существующих протоколов передачи данных;
- управление интернет – программами;
- фильтрация личной и коммерческих электронных писем;
- оценка интернет-трафика от беспроводных систем;
- классификация безопасности FTP – соединения.

2. Используемые данные - защита медийной информации, используемой сотрудниками учебного заведения.

3. Отдых данных: защита данных, хранящихся в памяти компьютерных устройств, хранящихся на рабочих местах или на серверах и в сетях хранения данных (сетях хранения).

Система DLP для определения уровня конфиденциальности образовательной информации основана на нескольких методах:

- лингвистический анализ отправляемых данных;
- анализ статистики интернет-трафика;
- идентификация шаблонных выражений;
- нанесение отпечатков пальцев на секретные документы.

1.2 Техническая характеристика системы «Инспектор»

Централизованная система управления деятельностью в области информационных технологий (далее - СУДО), состоящая из системы контроля и надзора за реализуемыми программами, сбора информации об установленных устройствах и системы отчетности.

Согласно анализу, проведенному в ТОО "PC4U", количество компьютеров должно составлять 185, система должна быть способна

контролировать не менее 200 пользователей и обладать следующими функциями:

Общие требования к управлению и отчетности ШУРС:

1. единой консоли отчетности в рамках системы, реализованной через веб-приложение;

2. ролевая система управления с возможностью делегирования управленческих полномочий и отчетности в соответствии со структурой организации;

3. панель управления в консоли управления, отображающая процессы, выполняемые на ПК в режиме реального времени;

4. генерировать SMTP-уведомления для оповещения о действиях при активации определенных конфигурируемых событий;

5. система должна обладать следующими характеристиками:

- мониторинг активного времени работы компьютера сотрудника;
- мониторинг программ;
- составление отчетов на посещенных веб-сайтах;
- мониторинг текстового сообщения;
- мониторинг операций файловых менеджеров;
- журнал скриншотов (скриншот рабочего стола за определенный период или действие);
- мониторинг печатных документов;
- мониторинг контроль действий и подозрительной деятельности устройств;
- формирование отчетности.

6. Архитектура системы должна предусматривать аппаратную и программную часть сервера (серверного модуля) и программную часть (клиентских модулей) - агентов для ПК.

7. Консоль управления - должна быть реализована в двух версиях: веб-приложение для создания отчетов и консоль управления (отдельное программное обеспечение для управления, установленное на рабочей станции ответственного сотрудника) для управления конфигурацией системы.

Требования к модулю для контроля использования данных SDCS:

1. Серверный модуль - должен позволять отображать информацию о действиях на компьютерах в режиме реального времени через веб-интерфейс и формировать отчеты следующим образом:

- время прихода/ухода сотрудника, диаграмма активности в течение дня;
- список посещаемых сайтов (отображение активной/пассивной работы с ними);
- использование программ (отображение активной/пассивной работы с ними);
- контроль распечатываемых документов;

- контроль электронной почты и почтовых вложений;
- мониторинг вводимого текста в программах, на сайтах;
- мониторинг ПО предназначенного для чатов;
- мониторинг операций с файлами, теневое копирование отправляемых через интернет и выводимых на флэш накопитель файлов;
- мониторинг поисковых запросов (Yahoo!, Yandex, Google, Bing);
- мониторинг графики в текстовом редакторе и буфере обмена;
- статистика о подозрительных действиях пользователей (запуск нежелательного программного обеспечения, посещение сайтов и т.д.);
- активный ответ на подозрительные действия (публикация сообщения о несанкционированных действиях и внесение результата в базу данных);
- создание сводных отчетов и различных критериев;
- отчеты можно экспортировать в Excel;
- возможность удаленного управления (удаленная установка клиентского ПО);
- хранение информации в собственной базе данных;
- возможность создания группы отчетов;
- настольный мониторинг в режиме реального времени;

2. Серверный модуль должен иметь аппаратную платформу для выполнения всех необходимых функций.

3. Агент для ПК (клиентского модуля) - должен быть установлен на клиентских компьютерах и отвечать следующим требованиям:

- имеют встроенную память со сроком хранения до 36 часов в автономном режиме (без подключения к локальной компьютерной сети, через которую серверный модуль доступен);
- сбор информации о действиях, выполняемых на персональном компьютере, на котором установлен клиентский модуль, и передача их в серверный модуль по локальной компьютерной сети через настроенный порт.
- агенты для ПК должны обеспечивать полную совместимость с операционными системами: - MicrosoftWindows® 8/7/Vista/XP/2000 NT 4.0 (SP6), Server 2000, Server 2003 (32-bit & 64-bit), Server 2008 (32-bit & 64-bit), Server 2008 (32-bit & 64-bit), Server 2008 R2, Server 2012.

4. Агенты ПК должны разрешать установку и работу на рабочих станциях с 128 МБ оперативной памяти для Windows 2000, Windows XP и Windows XP.

5. Административная консоль должна предоставлять параметры сервера и клиента, а параметры клиента должны быть разделены на следующие группы:

- в случае компьютеров: конфигурация принимается компьютерами, но не пользователями, так как на одном компьютере могут работать несколько пользователей;
- для пользователей: конфигурации, которые принимаются отдельными пользователями компьютеров, но не самими компьютерами.

Производители систем мониторинга и управления ПК отвечают этим требованиям: InfoWatch, SearchInform, NeoSpy и Инспектор.

Таблица 2 - Для сравнения производителей систем мониторинга и управления на базе ПК

Название системы	InfoWatch	SearchInform	NeoSpy	Инспектор
Модульность системы	Нет	Да	Нет	Нет
Места установки	Сервер, клиент	Сервер, клиент	Сервер, клиент	Сервер, клиент
Лицензирование	Каналы перехвата, технологии анализа	Сервер, mail, IM, Skype, Print, device, HTTP, FTP	Сервер, mail, IM, Skype, Print, device, HTTP, FTP	Сервер, mail, IM, Skype, Print, device, HTTP, FTP
Роли	Несколько	Любое количество	Одна	Несколько
Контроль IM	Да	Да	Текст	Да
Контроль HTTP/HTTPS, FTP	Да	Да	Да	Да
Контроль Skype	Текст	Да	Текст	Да
Контроль E-mail	Да	Да	Текст	Да
Социальные сети и блоги	Да	Да	Текст	Да
Контроль подключаемых внешних устройств	Да	Да	Да	Да
Контроль портов	USB,COM,LPT, Wi-Fi, Bluetooth	USB, LPT	USB	USB,COM,LPT, Wi-Fi, Bluetooth
Блокируемые протоколы	HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S, IMAP4	SMTP, POP3, MAPI, IMAP, HTTP,FTP, ICQ, Jabber	SMTP, POP3, MAPI, IMAP, HTTP,FTP, ICQ	HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S, IMAP4
Анализ по словарю	Да	Да	Нет	Да
Лингвистический анализ	Да	Да	Нет	Да
Анализ транслита	Да	Нет	Нет	Да
Анализ архивов	Да	Да	Нет	Да
Анализ рисунков	Да	Да	Нет	Да
Предустановленные шаблоны фильтрации	Да	Да	Да	Да
Задержка отправки подозрительных сообщений	Да	Да	Нет	Да
Логирование действий администраторов системы	Да	Да, при приобретении отдельного модуля	Нет	Да

Продолжение таблицы 2

Название системы	InfoWatch	SearchInform	NeoSpy	Инспектор
Режим установки агентов	Да	Да	Нет	Да
Защита агентов от выключения	Да	Да	Да	Да
Запись отчетов в локальное хранилище в случае недоступности сервера	Да	Да	Да	Да
Просмотр истории инцидентов	Да	Да	Да	Да
Режимы оповещений	Консоль, почта	Консоль, почта, графики	Почта	Консоль, почта
Возможность тестирования продукта на серверах разработчика	Нет	Нет	Нет	Нет
Возможность получения демо-версии для тестирования внутри организации	Нет	Нет	Нет	Нет
Необходимость приобретения оборудования для обработки и хранения данных	Да	Да	Да	Нет
Цена для компании 200 ПК (тг.)	25 000 000	20 000 000 - 30 000 000	1 117 500	с годовой поддержкой

Согласно проведенному анализу, в качестве оптимального способа защиты ИС был выбран отечественный продукт ТОО АПК "Инспектор" ПК4У, который имеет определенные преимущества и не уступает другим аналогичным продуктам.

1) Первый критерий заключается в том, что, в отличие от всех других производителей, Инспектор не требует приобретения оборудования для обработки и хранения данных или дополнительного программного обеспечения (операционная система, база данных).

2) Инспектор поддерживает морфологию казахского языка, которая играет важную роль во внедрении этой системы в любой организации в Казахстане.

3) Поскольку инспектор АПК является национальным продуктом, производитель предпочитает, чтобы продукт был доступен для обучения в рамках данного тезиса. Внедрение поддержки со стороны местных разработчиков оказывает значительное влияние на внедрение продукта. С экономической точки зрения агропромышленный комплекс "Инспектор" выгодно использовать, рассмотрение других продуктов возможно из-за их высокой стоимости только при рассмотрении временно ограниченных демонстрационных вариантов.

Вывод по второй главе. Вторая глава дипломной работы посвящена анализу технических и дополнительных характеристик предприятий-производителей систем мониторинга и контроля действий пользователей на ПК: InfoWatch, SearchInform, NeoSpy и Инспектор. Согласно проведенному анализу, оптимальным методом защиты информации был выбран отечественный продукт "Инспектор". Разработаны технические требования по внедрению продукта "Инспектор" в производственную среду ТОО "PC4U". Данный продукт совместим с внутренними системами защиты информационных систем компании: ActiveDirectory, Антивирус Касперского и KerioWinrouteFirewall.

Программно-аппаратный комплекс Инспектор представляет собой комплексное решение для защиты важной конфиденциальной информации, систему контроля и отслеживания действий, совершаемых на компьютере пользователем. Информация о важных параметрах и особенностях продукта "Инспектор" и его преимуществах приведена выше.

В целом, эта глава работы посвящена обоснованию выбранного оптимального метода, его анализу и исследованию и составлению технических требований по внедрению системы мониторинга и контроля на ПК "Инспектор" в ТОО "PC4U" в третьей главе.

2 Внедрение аппаратно-программного решения и разработка рекомендации по снижению рисков в информационной системе предприятия.

2.1 Внедрение и реализация системы мониторинга «Инспектор» в ИС ТОО«PC4U»

Первой стадией внедрения системы мониторинга «Инспектор» являлось заполнение опросного листа в соответствии с разработанной ранее технической спецификаций системы. На основании предоставленных данных компания-производитель выполнила первоначальные настройки параметров системы.

Процесс внедрения «Инспектор» в информационную среду ТОО PC4U составляет 3 этапа:

1. установка серверного комплекса;
2. установка клиентского модуля;
3. выполнение настроек комплекса.

Первый этап. «Установка серверного модуля комплекса» является относительно несложным, так как достаточно установить оборудование аппаратно-программного решения и подключить к локальной компьютерной сети и электропитанию. После выполнения данных процедур с ПК администратора была проверена доступность административного интерфейса серверной части комплекса через компьютерную сеть. После того, как убедились, что все службы работают: доступна консоль управления и административная часть, была выполнена установка серверной части.

Второй этап. «Установка клиентской части», которая выполняет наблюдение за ПК и передает данные на серверный модуль. На этапе инсталляции была установлена клиентская часть на один локальный компьютер, после проверки сбора данных серверным модулем и формирования отчета была установлена на удаленные компьютеры с помощью программы ActiveDirectory.

При установке на локальный компьютер была автоматически запущена программа настроек агента с запросом IP адреса серверного модуля АПК Инспектор. После указания адреса установка клиентской части была завершена, при этом в системе не произошло никаких видимых изменений. После установки системы на локальный компьютер была произведена проверка поступления данных на серверный модуль комплекса АПК. Для этого был выполнен вход в административную панель комплекса и проверены данные в модулях «Онлайн» и «Оффлайн».

Пошаговая установка клиентского модуля:

1) копирование установочной программы на рабочий экран пользователя (рисунок 1);

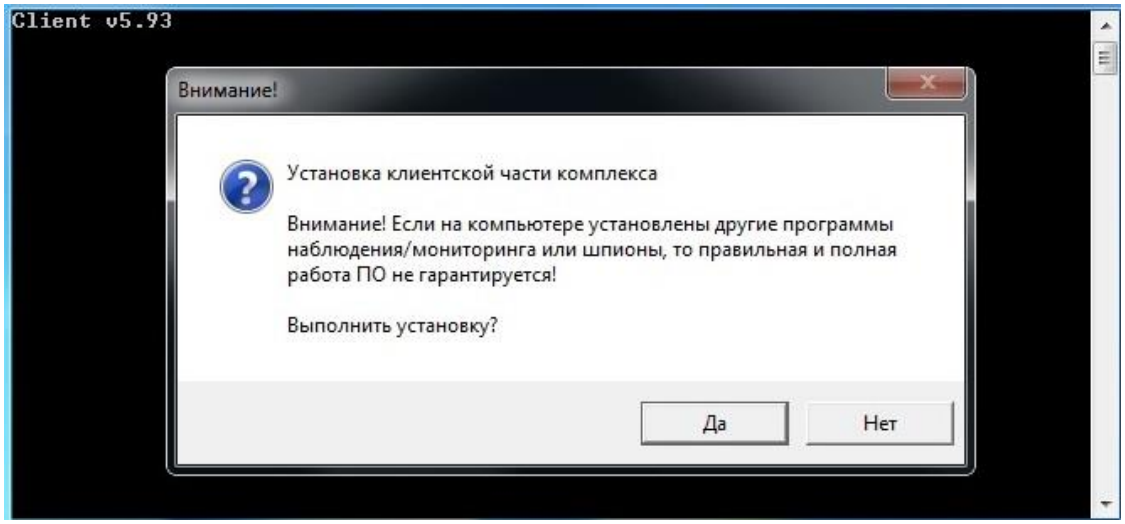


Рисунок 1 – Запрос при процессе установки системы

2) Далее вводим IP адрес серверной машины (рисунок 2):

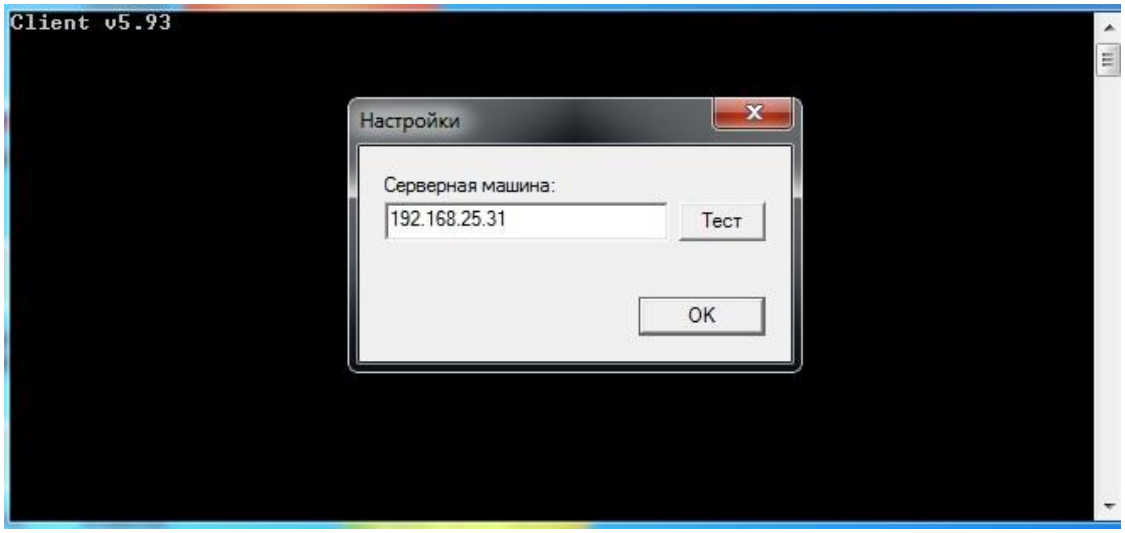


Рисунок 2 – Введение IP адреса серверной машины

3) Завершение установки программы (рисунок 3):

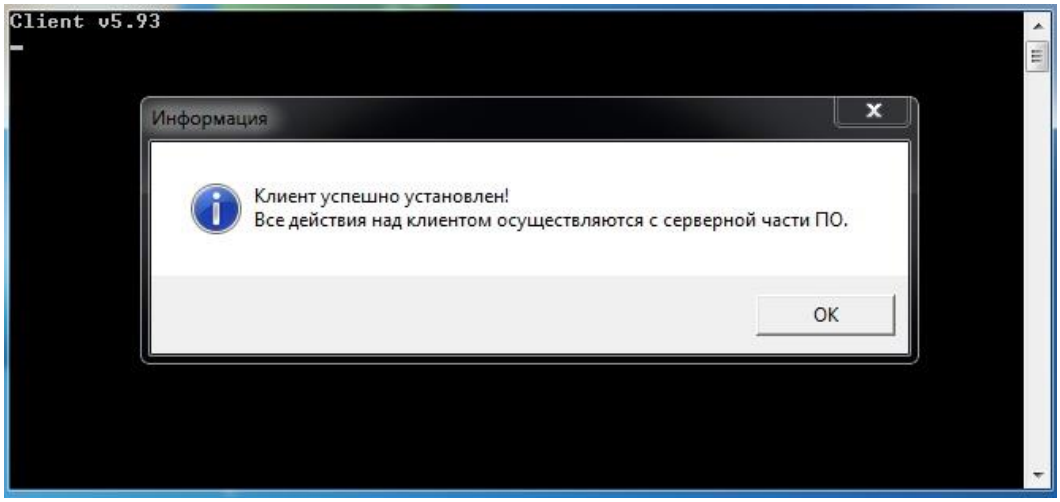


Рисунок 3 – Завершение установки клиентской части

Далее была произведена автоматическая установка на группы компьютеров с помощью службы MicrosoftActiveDirectory. Для этого были подготовлены два установочных пакета агентского модуля для 32 и 64-х бит системы.

Для выполнения процедуры установки под учетную запись администратора домена были выполнены следующие действия:

1) были размещены 2 установочных пакета в папке с открытым общим доступом по локальной сети;

2) в консоли управления ActiveDirectory была настроена новая «Групповая политика» настроек созданной новой организационной единицы, в которой был добавлен список установленных программ с инсталляционными пакетами агентского модуля с заданными IP адресами с серверного модуля. После этого была выполнена перезагрузка некоторых

тестируемых ПК и проверена их появление и доступность в системе Инспектор.

Второй этап «Выполнение настроек комплекса». Для более правильной работы были выполнены базовые настройки АПК Инспектор. Были настроены права административного пользователя, который имеет возможность наблюдать в режиме «Онлайн» и «Оффлайн» за всеми сотрудниками организации. Далее были выполнены настройки комплекса, которые делятся на серверные и клиентские Серверные настройки предназначены для серверного модуля, а клиентские настройки предназначены для пользователей ПК, подключенных к серверному модулю, которые передает настройки клиентским компьютерам при их включении и их работе. Клиентские настройки делятся: на группы для компьютера, пользователей и группы.

Настройки для компьютеров предназначены и воспринимаются ПК, но не их пользователей, так как на одном ПК могут работать несколько пользователей.

Настройки для пользователей предназначены и воспринимаются отдельными пользователями ПК.

Настройки группы предназначены для определенных групп пользователей и компьютеров.

Основными серверными настройками являются общие настройки, где указываются период хранения отчетов. При инсталляции системы был установлен период хранения пользовательских отчетов данных: 90 дней. Далее были выполнены клиентские настройки для компьютеров и пользователей. Основные настройки, которые потребовали внимания – это настройки локального хранилища: локальная база данных АПК Клиента, которая выполняет режим черного ящика при отсутствии соединения с серверной частью комплекса (все данные наблюдения накапливаются в базе данных до соединения с сервером). В данном типе настроек был установлен период – 48 часов.

Наиболее важной опцией являются настройки системы мониторинга «Снимки экранов». Была произведена настройка на осуществление снимков каждые 10 минут.

Также в серверной части был установлен «анализатор рисков, который предназначен для выявления возможных рисков организации. Данный отчет проводит анализ всей ранее собранной информации на ПК и показывает существующие риски и события, на основании которых эти риски были определены. А также наглядно показывают программы, в которых работает пользователь, что дает возможность оценки его работы. Для этого были созданы словари «Рабочий», где указаны Интернет-ресурсы и программы, относящиеся к рабочей профессиональной деятельности.

2.2 Анализ результатов внедрения системы «Инспектор»

Система мониторинга и контроля действия была установлена в 15 рабочих компьютерах сотрудников 13 марта. Основные функции системы

заключались в выполнении мониторинга запущенных программ, приложение и веб-сайтов на рабочих персональных компьютерах сотрудников, в осуществлении перехвата сообщений, снимков экрана монитора, мониторинг вводимых пользователем текстов и всех других действий на ПК, необходимые для информационной защиты и контроля.

Функции и действия, выполняемые системой, дают службе безопасности возможности:

– увеличить контроль и роль службы;

– мониторинг и контроль подозрительных действий;

– предотвратить утечку важной конфиденциальной информации;

– получить полную информацию при случаях потери или попыток получения информации;

– найти факты хищения данных и возможности защититься от них.

При запуске системы мониторинга и контроля доступа «Инспектор» в общих настройках были заданы следующие параметры:

– рабочий день – 8 часов;

– начало времени рабочего дня – 09:00;

– перерыв в течение дня – 1 час.

С 13.03.2017 по 04.04.2017 г. был проведен анализ работы системы мониторинга «Инспектор» на рабочих компьютерах 15 сотрудников организации ТОО PC4U.

При запуске мастера отчетов на окне появляются следующие формы получения отчета результатов (рисунок 4):

Рисунок 4 – Формы представления отчета результатов

– сформирование отчета в новом окне с активными функциями;

– получение и автоматическое скачивание отчета по полученным результатам в виде архивной папки;

– поиск необходимой информации по словам и выражениям в отчете.

При формировании отчета в новом окне формируется его меню, где отображаются все необходимые данные по действиям сотрудников. Мастер отчетов системы в Оффлайн режиме содержит категории: категории/отклонения, анализатор рисков, сводный отчет, машинное время, пользовательское время, рабочие программы**,** посещаемые сайты, буфер обмена, интернет-запросы, снимки экранов, печать на принтере, файловые операции, отправка файлов, письма (e-mail), чаты и звонки, контакты, граф

связей, события по пользователю и компьютеру, оборудование/софт, установки программ.

По проведенному анализу системы «Инспектор» были получены результаты по следующим категориям:

1) категории-отклонения дают возможность в общей таблице увидеть активное время сотрудника, время в программах, в интернете, развлечения, поиск работы, рабочие, объем информации набранного текста, количество отправленных файлов, событий.

Категории | Отклонения | Ресурсы

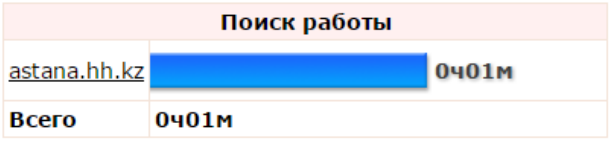
	Всего	Среднее	Минимум	Максимум
Активное время	75ч56м	75ч56м	75ч56м	75ч56м
Время в программах	41ч52м	41ч52м	0ч01м	41ч52м
Время в интернете	21ч34м	21ч34м	0ч01м	21ч34м
Прочее	36ч17м	36ч17м	0ч01м	36ч17м
Развлечения	8ч06м	8ч06м	0ч33м	8ч06м
Поиск работы	0ч01м	0ч01м	0ч01м	0ч01м
Рабочие	19ч04м	19ч04м	0ч01м	19ч04м
Набрано текста	511.5 KB	511.5 KB	511.5 KB	511.5 KB
Напечатано	70	70	70	70
Отправлено файлов	86	86	86	86
События	56	56	56	56

Рисунок 5 – Анализ категории системы «Инспектор»

На рисунке выше отображен общий анализ использования времени сотрудниками организации. По полученному анализу видно, что больше времени сотрудник проводит в программах, в интернете и прочих программах.

При установлении фиксированной времени работы сотрудника по категориям можно учитывать любое превышение времени работы от установленной нормы и получать отчет в графе «Отклонения».

Развлечения	
vk.com	5ч08м
youtube.com	1ч54м
"Mail.Ru Агент"	0ч33м
instagram.com	0ч19м
facebook.com	0ч14м
Всего	8ч06м



Поиск работы	
astana.hh.kz	0ч01м
Всего	0ч01м

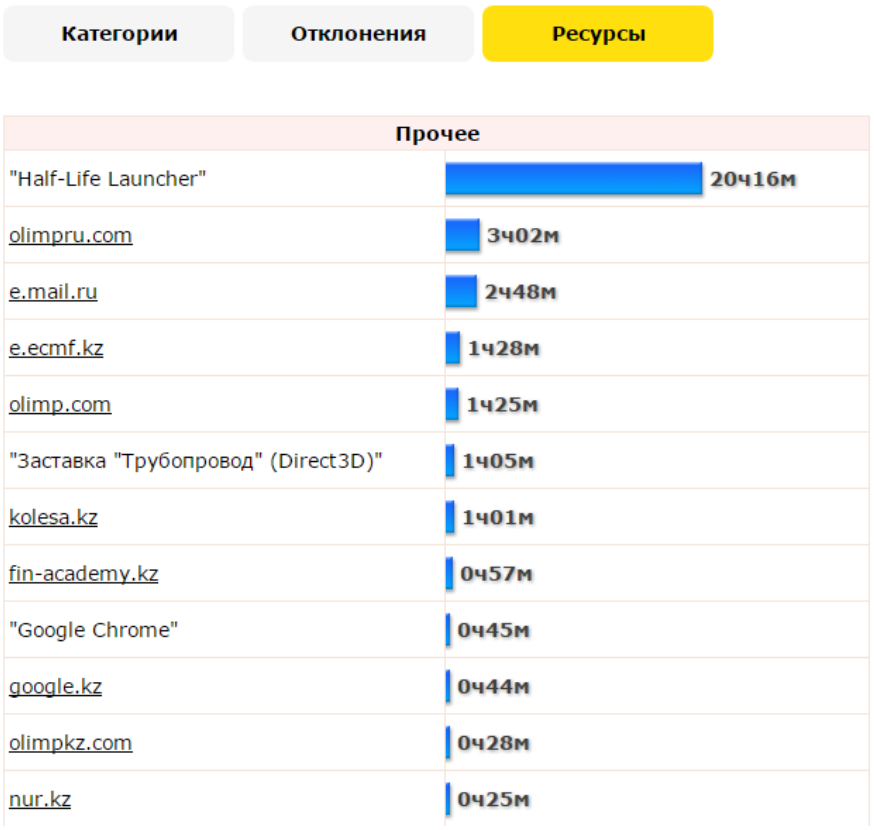


Рисунок 6 – Анализ количества времени использования информационных ресурсов

По отчету максимальное рабочее время сотрудник тратит на прочие ресурсы, что показывает неэффективное использование рабочего времени и возможность появления различных рисков как для ПК, так и для общей работы организации.

Анализатор рисков – анализ эффективной, неэффективной или вредной работы сотрудника организации:

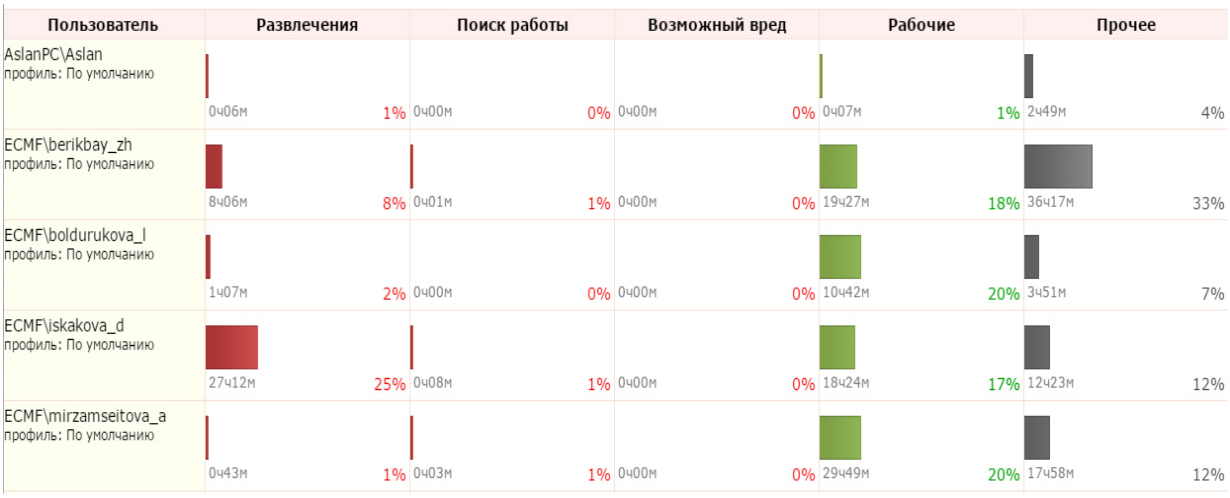


Рисунок 7 – Анализатор рисков

По полученному отчету можно сделать вывод, что особо важных рисков не наблюдалось.

Сводный отчет – отчет, содержащий наглядную общую статистику в области используемых ресурсов по сотрудникам на ПК.

Прогулы(*)	Время на работе	Время в программах	Время в интернете	Популярные
прогулов: 5 приход ранее на 0ч29м уход позднее на 2ч38м	140% 156ч48м	**38%** 42ч16м	**20%** 21ч34м	"Half-Life Launcher" (19%, 20ч16м) "Microsoft Office Excel" (14%, 15ч40м) "Microsoft Office Word" (2%, 1ч58м) "Проводник" (2%, 1ч25м) "Заставка "Трубопровод" (Direct3D)" (1%, 1ч05м) все прочие (2%, 1ч54м) vk.com (5%, 5ч08м) olimpru.com (3%, 3ч02м) e.mail.ru (3%, 2ч48м) youtube.com (2%, 1ч54м) e.ecmf.kz (2%, 1ч28м) все прочие (7%, 7ч18м)

Рисунок 8 – Общая статистика используемых ресурсов

Машинное время – время активной работы ПК по настраиваемой дате.

День	Время работы	% рабочего дня	Первое включение	Последнее выключение
2017-03-13 (ПН)	8ч40м	**109%**	09:26	18:10
2017-03-14 (ВТ)	13ч25м	**168%**	10:41	00:04
2017-03-15 (СР)	18ч15м	**228%**	00:04	18:22
2017-03-16 (ЧТ)	9ч50м	**123%**	09:27	19:15
2017-03-17 (ПТ)	11ч20м	**142%**	09:20	20:38
2017-03-18 (СБ)	10ч25м	**130%**	08:58	19:21
2017-03-27 (ПН)	14ч20м	**179%**	09:46	00:04
2017-03-28 (ВТ)	19ч40м	**246%**	00:04	19:42
2017-03-29 (СР)	9ч45м	**122%**	09:09	18:51
2017-03-30 (ЧТ)	10ч15м	**128%**	09:15	19:27
2017-03-31 (ПТ)	10ч20м	**129%**	09:01	19:19
2017-04-01 (СБ)	5ч00м	**63%**	13:30	18:26
2017-04-03 (ПН)	8ч10м	**102%**	11:01	19:08
2017-04-04 (ВТ)	7ч45м	**97%**	09:17	16:59

Рисунок 9 – Анализ машинного времени

По полученному результату можно сказать, что сотрудники иногда не отключают компьютеры на своих рабочих местах, что также может быть источником сбоев работы ПК, вести к утечке конфиденциальной информации и к финансовым потерям.

Программы – список используемых программ и время просмотра данных программ.

#	Заголовок окна приложения	Активное время	Общее время
	Counter-Strike "Half-Life Launcher" %SystemDrive%\Counter-Strike 1.6 Chrome v1.4.9\hl.exe 2017-03-13 10:05:44, 2017-03-14 12:42:04, 2017-03-15 13:42:20, 2017-03-16 13:38:53, 2017-03-17 12:20:15, 2017-03-18 10:15:25, 2017-03-27 11:11:50, 2017-03-28 11:50:38, 2017-03-29 09:23:22, 2017-03-30 09:32:19, 2017-03-31 12:54:16, 2017-04-01 15:40:12, 2017-04-03 13:45:06, 2017-04-04 09:30:49, 2017-04-04 11:29:21, 2017-04-04 14:29:47, 2017-04-04 14:53:52 Показать/скрыть вводимый текст	**19%** (20ч16м)	19% (20ч29м)
	Microsoft Excel "Microsoft Office Excel" %ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE 2017-03-13 09:38:03, 2017-03-15 15:13:26, 2017-03-16 11:24:29, 2017-03-17 12:04:48, 2017-03-27 10:11:52, 2017-03-28 14:24:25, 2017-03-29 10:29:31, 2017-03-30 10:18:27, 2017-03-31 11:30:15, 2017-04-03 14:33:28, 2017-04-04 09:23:18, 2017-04-04 12:27:50, 2017-04-04 12:29:10 Показать/скрыть вводимый текст	**6%** (6ч42м)	8% (8ч58м)
	Microsoft Excel - Том 18 Регистр.2016г. "Microsoft Office Excel" %ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE 2017-04-03 12:54:07, 2017-04-04 11:06:01, 2017-04-04 15:35:23	**2%** (1ч59м)	3% (2ч26м)

Рисунок 10 – Анализ отчета по часто-используемым программам

По полученному результату анализа работы одного из сотрудников видно, что большее время один из сотрудников организации проводит за просмотром прочих программ, таких как Counter-Strike 19%.

Буфер обмена – сохранение передаваемых текстов, файлов и картинок. При случае возникновения инцидентов или подозрительных действий по ИБ, можно проанализировать и увидеть кем, кому и какие материалы были отправлены.

[2017-03-13 10:03:40] Конысова Гульзахира Бахадыровна Конысова Гульзахира Бахадыровна
...
[2017-03-13 10:03:44] Конысова Гульзахира Бахадыровна Конысова Гульзахира Бахадыровна Договор № у от 02.03.2017 г.
Адрес: РК, г. Астана, ул.
ИИН
Уд.личности №
Выдано 230455
87015447101
Gb-astana@mail.ru

...
[2017-03-13 10:03:57] Конысова Гульзахира Бахадыровна Конысова Гульзахира Бахадыровна Договор № у от 02.03.2017 г.
Адрес: РК, г. Астана, ул.
ИИН
Уд.личности №
Выдано 230455
87015447101
Gb-astana@mail.ru

...
[2017-03-13 10:34:45] Акционерно общество «Национальная компания «Казахстан Инжиниринг»
...
[2017-03-13 10:35:24] (Kazakhstan Engineering)
...
[2017-03-13 10:43:12] 620300226777
...
[2017-03-13 10:43:42] 030440000693
...
[2017-03-13 10:59:18] 030440000693

Рисунок 11 – Анализ отчета буфера обмена

Печать на принтере – возможность перехвата распечатанных файлов.

Пользователь	Время	Страниц	КБайт	Бумага	Цвет	Документ
ECMF\iskakova_d Всего страниц: **190**	2017-03-13 09:27	1	176 КБ	A4 210x297	-	*Том 12 Регистр.2016г..xlsx* 2017-03-13_09-27-31_00003.spl 2017-03-13_09-27-31_00003.shd 2017-03-13_09-27-31.jpg
	2017-03-13 10:56	56	6904 КБ	A4 210x297	-	*Microsoft Word - НН _вечер гр.с 13-20.03., 24.03.17_ .d* 2017-03-13_10-56-08_00004.spl 2017-03-13_10-56-08_00004.shd 2017-03-13_10-56-08.jpg 32B1F959.docx
	2017-03-13 10:57	1	143 КБ	A4 210x297	-	*Microsoft Word - Анкета №1.doc* 2017-03-13_10-57-32_00005.spl 2017-03-13_10-57-32_00005.shd 2017-03-13_10-57-32.jpg 32B1F959.docx
	2017-03-13 10:58	1	94 КБ	A4 210x297	-	*Microsoft Word - заявление на экзамен 2017.docx* 2017-03-13_10-58-53_00006.spl 2017-03-13_10-58-53_00006.shd 2017-03-13_10-58-53.jpg 32B1F959.docx
	2017-03-13 11:00	1	65 КБ	A4 210x297	-	*Microsoft Word - обьявление.docx* 2017-03-13_11-00-23_00007.spl 2017-03-13_11-00-23_00007.shd 2017-03-13_11-00-23.jpg обьявление.docx
	2017-03-13 11:01	1	65 КБ	A4 210x297	-	*Microsoft Word - обьявление.docx* 2017-03-13_11-01-06_00008.spl 2017-03-13_11-01-06_00008.shd 2017-03-13_11-01-06.jpg обьявление.docx

Рисунок 12 – Анализ отчета по распечатанным документам

При обнаружении утечки какой-нибудь важной информации по данному отчету можно отследить распечатанные файлы, которые могут быть каналом

утечки информационных ресурсов. В полученном отчете имеется полная информация о распечатанном документе: количество страниц, размер документа и бумаги, время распечатывания.

Файловые операции – осуществление перехватов копирования, удаления, переноса файлов. При копировании файлов на флэшку возможно теневое копирование.

Пользователь	Время	Файл/Информац
ECMF\tkach_n Всего файлов: **29**	2017-03-14 11:26	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Письмо пригл Внутр ау https://e.mail.ru/compose/14893996030000000093/reply/
	2017-03-14 11:26	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Программа_Внутренни https://e.mail.ru/compose/14893996030000000093/reply/
	2017-03-15 10:25	C:\Users\tkach_n\Desktop\Сертификация аудиторов гос.заказ\Протоколы\results (1).xls https://e.mail.ru/compose/?1489551829093
	2017-03-15 10:30	C:\Users\tkach_n\Desktop\Сертификация аудиторов гос.заказ\Протоколы\results (1).xls https://e.mail.ru/compose/?1489551829093
	2017-03-15 14:57	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Коммерческое гос.аудит 2017.PDF https://e.mail.ru/compose/14895678540000000188/reply/
	2017-03-15 15:02	C:\Users\tkach_n\Desktop\Правила на 07.02.17.v1500012720.09-12-2016.rus.docx https://e.mail.ru/compose/14895678540000000188/reply/
	2017-03-15 16:04	C:\Users\tkach_n\Desktop\Внутренний-аудит для Натали.jpg https://e.mail.ru/compose/?1489572127430
	2017-03-16 09:15	C:\Program Files\Google\Chrome\Application\chrome.exe (chrome.exe)
	2017-03-16 09:15	C:\Program Files\Google\Chrome\Application\chrome.exe (chrome.exe)
	2017-03-17 10:07	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Документы к семинару https://e.mail.ru/compose/?1489723625427
	2017-03-17 10:43	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Документы к семинару https://e.mail.ru/compose/?1489723625427
	2017-03-17 10:43	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Документы к семинару https://e.mail.ru/compose/?1489723625427
	2017-03-17 10:43	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Документы к семинару https://e.mail.ru/compose/?1489723625427
	2017-03-17 10:44	C:\Users\tkach_n\Desktop\КОММЕРЧЕСКИЕ КУРСЫ\2017\Внутренний аудит\Документы к семинару https://e.mail.ru/compose/?1489723625427

Рисунок 13 – Анализ отчета по файловым операциям

При обнаружении каких-нибудь инцидентов ИБ можно определять и находить важные документы по файловым операциям, где имеется полная информация об операциях с файлами и документами. Определение типа операции: копирование, удаление, перенос и время обработки файла.

Письма (e-mail), в которых осуществляется перехват входящих и исходящих электронных почтовых писем.

Пользователь	Время	I/O	От кого/Кому	Файл/Информация
ECMF\mirzamseitova_a Всего писем: **165**	2017-03-13 09:24		Чудо-очки Zoom HD ywwedyy@informazion.eu	2017-03-13_09-24-13_0.msg (280 KB) *Очки для мелких и точных работ. Увеличение 160%*
	2017-03-13 09:24		Чудо-очки Zoom HD ajrizxd@informazion.eu	2017-03-13_09-24-13_1.msg (280 KB) *Очки для мелких и точных работ. Увеличение 160%*
	2017-03-13 09:24		ecmf dmf@ecmf.kz	2017-03-13_09-24-13_2.msg (40 KB) *Подана заявка на обучение*
	2017-03-13 09:24		andrii@publisher12.ru	2017-03-13_09-24-13_3.msg (40 KB) *ТОО Мир научных публикаций. Алматы.*
	2017-03-13 09:24		7131471@mail.ru	2017-03-13_09-24-13_4.msg (2564 KB) *Fwd: Предварительная налоговая проверка, бухгалтерское и налоговое сопровождение от Корпорации "ЗУМРАД*
	2017-03-13 13:21		Витрина духов info@filamest.eu	2017-03-13_13-21-20_0.msg (136 KB) *Витрина духов Тушь В ПОДАРОК*
	2017-03-13 15:53		umc_astana@mail.ru	2017-03-13_15-53-10_0.msg (1912 KB) *Приглашение на семинар "Повышение квалификации для профессиональных бухгалтеров*
	2017-03-13 15:54		gulnarsga@mail.ru	2017-03-13_15-54-51_0.msg (1904 KB) *Приглашение на семинар "Повышение квалификации для профессиональных бухгалтеров*
	2017-03-13 15:59		aigul_shaimahova@mail.ru	2017-03-13_15-59-41_0.msg (1908 KB) *Приглашение на семинар "Повышение квалификации для профессиональных бухгалтеров*
	2017-03-13 16:00		g.shomayeva@sk.kz	2017-03-13_16-00-18_0.msg (1908 KB) *Приглашение на семинар "Повышение квалификации для профессиональных бухгалтеров*
	2017-03-13 16:03		unknown@recipient	2017-03-13_16-03-33_0.msg (1920 KB) *Приглашение на семинар "Повышение квалификации для профессиональных бухгалтеров*

Рисунок 14 – Анализ отчета по письмам (e-mail)

При обнаружении каких-нибудь инцидентов ИБ можно определять и находить важные документы по письмам (e-mail), где имеется полная информация о передаваемых файлов и документах: адрес получателя, дата отправки, объем файла и ссылка на этот файл.

События: пользователь – запись в отчет событий, которые сотрудник может настроить. Данные события классифицируются по типу важности. Например, запуск программ, сайтов, ввод текста с учетом порядка неточного сравнения слов.

Пользователь	Время	Тип	Важность	Описание
ECMF\tkach_n	2017-03-13 14:59:44	⚠	●	запуск программы/сайта или ввод текста *"@CREDITCARD@:* 2017-03-13_14-59-44.jpg
	2017-03-13 17:47:41	⚠	●	Нетипичное поведение *"копирование в буфер обмена"* 2017-03-13_17-47-41.jpg
	2017-03-14 09:40:55	⚠	●	запуск программы/сайта или ввод текста *"@EMAIL@: natalia* 2017-03-14_09-40-55.jpg
	2017-03-14 11:26:36	ℹ	●	отправка файла(ов) по интернету 2017-03-14_11-26-36.jpg
	2017-03-14 11:42:39	⚠	●	запуск программы/сайта или ввод текста *"~начальник"* 2017-03-14_11-42-39.jpg
	2017-03-14 12:57:42	⚠	●	Нетипичное поведение *"копирование в буфер обмена"* 2017-03-14_12-57-42.jpg
	2017-03-15 10:25:14	ℹ	●	отправка файла(ов) по интернету 2017-03-15_10-25-14.jpg

Рисунок 15 – Анализ отчета по событиям пользователя

Снимки экранов. В настройках системы «Инспектор» были заданы настройки автоматических снимков экранов рабочего стола сотрудника через каждые 10 минут.

Рисунок 16 – Анализ отчета снимки экранов

В результате анализа ИС ТОО PC4U было выявлено несколько нарушений по работе сотрудников с ПК, с рабочими файлами и документами, программами и прочими интернет-ресурсами.

Нарушения были представлены следующими действиями и инцидентами информационной безопасности:

- сотрудники иногда не отключают компьютеры на своих рабочих местах, что может быть источником сбоев работы ПК, вести к утечке конфиденциальной информации и к финансовым потерям;
- печать на принтере и сканирование сотрудниками своих личных документов и прочих образовательных ресурсов;
- просмотр интернет-ресурсов (web-страниц, видео контента, прослушивание и скачивание музыки, включение онлайн-игр) в рабочее время;
- отключение антивирусного программного обеспечения без ведома системного администратора;
- общение через социальные сети (вконтакте, Facebook, мой мир, одноклассники, skype);
- скачивание и установка вредоносных программ (непреднамеренное нарушение).

После выявлений вышеизложенных нарушений с помощью системы мониторинг а и контроля действий «Инспектор» были приняты следующие меры:

- замечание руководителя в устной форме;
- сотрудники отдела были устно предупреждены о принятии более строгих мер в случае повторного нарушения;
- ограничение доступа сотрудников на часто посещаемые интернет-ресурсы (социальные сети) в рабочее время;
- ограничения по скорости интернет, доступа на несоответствующие информационные ресурсы.

По анализу полученных отчетов разработана концепция информационной безопасности, содержащая рекомендации по уменьшению количества уязвимостей и улучшению эффективности защиты информационно-образовательной системы ТОО PC4U.

Повторный анализ с интервалом 15 рабочих дней показал непосредственный рост результатов работы и качества распределения рабочего времени. Сотрудники организации эффективно начали использовать свое рабочее время, более серьезно подходить к выполнению своих обязанностей. Количество посещений социальных сетей и иных интернет ресурсов сократилось на 87%.

2.3 Разработка рекомендаций по минимизации рисков

В ходе написания диссертационной работы помимо внедрения АПК «Инспектор» в ТОО PC4U, был осуществлен анализ официального сайта

http://pc4u.kz/ данной учебной организации с помощью DLP системы. В результате этого анализа сделаны следующие выводы:

- опасный код на странице – Проблем не обнаружено;
- вирусы в скриптах – Проблем не обнаружено;
- вставки с опасных сайтов – Проблем не обнаружено;
- сайт в базе вредоносных – Проблем не обнаружено;
- ошибки страницы – Проблем не обнаружено;
- вставки с неизвестных сайтов – Проблем не обнаружено;
- ресурсы с внешних сайтов – Проблем не обнаружено;
- внешние ссылки – Проблем не обнаружено.

Основные недостатки, которые были обнаружены:

- тестирование на проникновение – обнаружены возможности применения ошибок и кода программного обеспечения для использования применения вредоносного кода или несанкционированного доступа;
- тестирование на стойкость авторизации – обнаружен недостаток защиты от повторного ввода паролей и возможности подбора паролей, скорость использования подбора пароля к одной учетной записи достаточно велика;
- не использовано SecureSocketsLayer (SSL) соединение, что свидетельствует о возможности перехвата данных;
- сайт уязвимStructured Query Language (SQL) атакам.

Протокол SSL является семейством протоколов для установки защищенного соединения между двумя лицами (организациями), обменивающихся данными.

Протокол SSL использует ассиметричную криптосистему с открытым ключом, созданную компанией RSA. Чаще всего SSL используется с широко применяемым и известным протоколом передачи гипертекста – http. О присутствии защищенного соединения можно узнать по наличию суффикса «s» (https). Протокол SSL обеспечивает защищенный обмен информацией за счет применения двух следующих элементов: аутентификация и шифрование.

Протокол SSL состоит из нескольких слоев:

- первый слой представлен транспортным протоколом TCP, где формируется пакет и осуществляется непосредственная передача информации по сети;
- второй слой представлен защитным слоем SSL RecordProtocol.

При защищенной передаче информации эти два слоя являются обязательными и составляют основу SSL, к которым в дальнейшем добавляются другие слои для усиления защиты. Для осуществления SSL соединения необходимо, чтобы сервер содержал установленный цифровой сертификат, идентифицирующий пользователей и серверы.

Наличие SSL соединения обеспечит предотвращение следующих действий:

- «спуфинг» (имитация соединения);

- несанкционированный доступ;
- разглашение конфиденциальной информации;
- изменение данных с корыстной целью.

Официальный сайт http://pc4u.kz/ уязвим SQLатакам. Это одна из наиболее распространенных атак прикладного уровня, применяемых в настоящее время в Интернете. Суть данных атак (инъекций) заключается во внедрении в данные произвольного SQL кода, которые могут привести к ошибочным запросам.

Ниже приведены результаты, подтверждающие уязвимость данного сайта:

1. Описание уязвимости. Внедрение SQL кода представляет собой уязвимость, позволяющая злоумышленнику изменять внутренние SQL-операторы путем манипулирования пользовательским вводом.

Обнаружено: Scripting (Blind_Sql_Injection.script).

Сведения об атаке

Фрагмент пути / <s> / <s> / <n> / [*] был установлен в 675 * 1 * 1 * 1 * 1 * 1 * 1 *

Проведенные тесты:

- 475' =>ERROR
- 475" =>ERROR
- 383*1*1* => ERROR
- 801*1*1*1*1 => OK
- 659*1*1*1*1* => ERROR
- 228*1*1*1*1*1*1 => OK
- 592*1*1*1*1*1*1* => ERROR

Исходное значение: 116

2. Описание уязвимости. Обнаружено: Scripting (Blind_Sql_Injection.script).

Сведения об атаке: URL-адрес, закодированный по URL-адресу POST, был установлен на if (now()=sysdate(),sleep(0),0) / *'XOR(if(now() = sysdate(), sleep(0),0)) OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Проведенные тесты:

- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'" XOR(if(now()=sysdate(),sleep(6),0))OR"*/ =>6.489 s
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'" XOR(if(now()=sysdate(),sleep(9),0))OR"*/ =>9.469 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'" XOR(if(now()=sysdate(),sleep(3),0))OR"*/ =>3.698 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'" XOR(if(now()=sysdate(),sleep(0),0))OR"*/ =>0.998 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'" XOR(if(now()=sysdate(),sleep(0),0))OR"*/ =>0.546 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'" XOR(if(now()=sysdate(),sleep(0),0))OR"*/ =>0.936 s

- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'" XOR(if(now()=sysdate(),sleep(0),0))OR"*/ =>0.624 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'" XOR(if(now()=sysdate(),sleep(6),0))OR"*/ =>6.474 s
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'" XOR(if(now()=sysdate(),sleep(0),0))OR"*/ =>0.577 s.

Исходное значение: образец% 40 email.tst

3. Длительный отказ в обслуживании пароля

Описание уязвимости. Отправляя очень длинный пароль (около 1000000 символов), можно привести к отказу в обслуживании на сервере. Данная проблема обычно вызвана уязвимой реализацией хеширования паролей. При отправке длинного пароля, процесс хэширования пароля приводит к выходу процессора и памяти.

Эта уязвимость влияет на / admin / auth / auth.

Открыто: Scripting (Long_Password_Denial_of_Service.script).

Сведения об атаке

Уязвимый пароль: passw.

Проведенные тесты:

- password of 1000000 characters => 28.798 s
- password of 100 characters => 0.453 s
- password of 100000 characters => 1.997 s
- password of 1100000 characters => 25.927 s
- password of 500 characters => 0.437 s

Рекомендации. Была проведена научно-исследовательская работа по изучению и анализу текущего состояния предприятия на базе ТОО PC4U. С учетом специфики работы был выбран и обоснован оптимальный метод базовой защиты ИС организации. В связи с тем, что сайт размещен за пределами организации на сторонней площадке и поддерживается сторонней компанией, рекомендуется обратиться к компаниям-разработчикам и хостинг-оператору для исправления замечаний и доработке программного кода с целью повышения организации информационной безопасности и защиты интернет-ресурса от хакерских атак. Рекомендуется использовать SSL соединение, также разработать положение по обеспечению безопасности интернет-ресурса, правила работы, а так же положение по резервному копированию сайта.

При защите сайта от SQL атак необходимо применять фильтрацию строковых параметров, фильтрацию целых чисел, ограничение входных параметров, применение запросов с определенными параметрами (подготовленные выражения).

Выводы по второй. Данная глава является рекомендательной, посвящена внедрению и реализации системы мониторинга «Инспектор» в ТОО PC4U, выполнен анализ результатов внедрения системы и приведены рекомендации по снижению рисков ИБ в информационно-образовательной системе вуза.

В результате анализа ИС ТОО PC4U было выявлено несколько нарушений по работе сотрудников с ПК, с рабочими файлами и документами, программами и прочими интернет-ресурсами. Руководителями организации были применены определенные меры по устранению замечаний, что в дальнейшем показало свой результат.

Система была оптимально настроена под производственное заведение ТОО PC4U. Внедрение АПК «Инспектор» позволило грамотно выстроить информационную безопасность, анализировать и оценить информационные ресурсы, данные, файлы, определить утечку важной информации к третьим лицам.

Также при анализе официального сайта ТОО PC4Uhttp://pc4u.kz/ были найдены уязвимые места:

- возможности применения ошибок и кода программного обеспечения для использования применения вредоносного кода или несанкционированного доступа;

- обнаружен недостаток защиты от повторного ввода паролей и возможности подбора паролей, скорость использования подбора пароля к одной учетной записи достаточно велика;

- не использовано SecureSocketsLayer (SSL) соединение, что свидетельствует о возможности перехвата данных.

Сайт уязвим Structured Query Language (SQL) атакам.

На основе полученных данных разработаны рекомендации по минимизации рисков информационной безопасности.

3 Оценка рисков информационной безопасности предприятия

Основание для осуществления работ по внедрению проекта «Инспектор».

По состоянию на 16.01.2018 г., в ТОО «PC4U» отсутствует полный контроль за действиями сотрудников в рабочее время на рабочем месте. Отсутствие автоматизированной системы контроля приводит к неконтролируемому использованию информационных ресурсов и данных ТОО «PC4U».

АПК «Инспектор» в АО ТОО «PC4U» внедряется в следующих целях:

- контролирование доступа к сети «Интернет»;

- контроль пользования информационными ресурсами ТОО «PC4U»;

- соблюдения трудовой дисциплины, режимов работы сотрудников за счет исключения использования информационных ресурсов и данных в личных интересах;

- автоматизация и минимизация однообразной работы отдела информационной безопасности;

- ограничения доступа работников в интернет в соответствии с их должностными обязательствами;

- автоматизирование учета рабочего времени сотрудников.

Введение в работу «Инспектор» в ТОО «PC4U» позволит осуществить следующие действия:

- полное отсутствие задержек при выполнении заказов по вине работников, использующих рабочее время не по назначению;
- оптимизация персонала, отвечающего за информационную безопасность в организации;
- обнаружение “простоя” в применении рабочего программного обеспечения.

Организованная работа АПК «Инспектор» при последующем его внедрении с глобальными настройками в ТОО «PC4U», принесет положительные аспекты в деятельность организации:

Для руководителей организации:

- получение наглядного и точного представления (статистики) о работе своих подразделений для анализа и разработки высокоэффективных мер по улучшению их функционирования;
- просмотр полных отчетов (об опаздываниях или ранних уходах, о работе сотрудников на определенный период).

Для отдела кадров организации:

- получение каждодневной актуальной информации по нарушителям порядка и политики ИБ, для быстрого принятия мер дисциплинарного и материального характера;
- назначение групповых политик доступа для структурных подразделений;

Для бухгалтерии:

- получение отчетов об отработанном работниками рабочего времени по установленному алгоритму;
- получение информации о времени отсутствия сотрудников на рабочем месте;
- получение информации об опаздываниях и ранних уходах персонала;
- контроль доступа чужих лиц к информационным данным бухгалтерии.

На основании вышеприведенной информации можно считать внедрение «Инспектор» в ТОО «PC4U» актуальной, экономически обоснованной задачей. Возмещение затрат на внедрение «Инспектор» осуществится за счет повышения уровня трудовой дисциплины сотрудников, оптимизации информационной защиты внутренней структуры организации и повышения эффективности работы руководителей структурных подразделений.

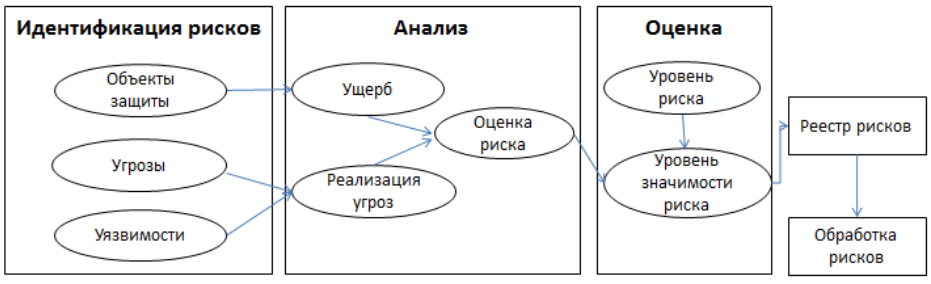


Рисунок 17 – Процесс оценки рисков информационной безопасности [28]

По степени критичности инциденты информационной безопасности классифицируют следующим образом: высокий, средний и низкий.

Таблица 3 – Оценка рисков информационной безопасности в АО «Финансовая Академия»

Степень тяжести последствий для деятельности организации	Вероятность возникновения опасности			
	Маловероятно (чрезвычайно редко, реже, чем раз в 5 лет)	Редко (реже, чем раз в год)	Возможно (каждый квартал-год)	Достаточно вероятно (каждый месяц-квартал)
Катастрофическая (прекращение деятельности организации)	С	С	В	В
Тяжелая (полная потеря невосстанавливаемой информации, застой работы, потеря имиджа)	Н	С	С	В
Средняя (потеря отдельных данных, разглашение конфиденциальной информации)	Н	Н	С	С
Легкая (нарушение целостности, вред документу, разглашение общедоступной информации)	Н	Н	Н	С
Степень риска	Меры по управлению рисками			
В (высокий)	Дальнейшее проведение работ сотрудниками организации невозможно без дополнительных мер по снижению риска. До возобновления работы сотрудников провести переоценку риска.			
С (средний)	Необходимо разработать меры по снижению риска.			
Н (низкий)	Риск приемлем. Дополнительные меры управления не требуются.			

По степени рисков ИБ активы производственных предприятии можно классифицировать следующим образом:

1 категория определяет высокую степень рисков:

- персональные данные сотрудников и клиентов;
- данные по техническим вопросам;
- коммерческая тайна (стратегия, политика, чтобы опережать другие предприятия);
- данные планово-финансового (бухгалтерского) отдела.

2 категория определяет среднюю степень рисков:

- производственные материалы, представляющие интеллектуальную собственность;
- официальный сайт http://pc4u.kz/ ;
- вирусы.

3 категория определяет низкую степень рисков:

- постановления предприятия;
- информационный блок;
- статистические и архивные данные.

4 Безопасность жизнедеятельности

4.1 Теоретическая часть

Комплексная система защиты информации на предприятии с использованием компьютерного оборудования и программного обеспечения. Для продуктивного рабочего процесса работника или работников необходимо обеспечить его или их оптимальными условиями для работы: удобными стульями или креслами, снижающих нагрузку на позвоночник; в меру просторным рабочим пространством, которое позволит работнику проделывать все необходимые действия и перемещения; разработка систем искусственного освещения, аспирационными системами, обеспечивающие вентиляцию воздуха и поддерживающие комнатную температуру на рабочем месте.

4.2 Рабочее помещения

При планировании рабочей зоны необходимо учитывать гигиенические свойства процессов, стандарты рабочей зоны и соотношение между техническими зонами и зонами оборудования и требуемой шириной прохода, чтобы обеспечить безопасную эксплуатацию и удобные методы и оборудование для технического обслуживания.

Рабочая зона расположена на втором этаже пятиэтажного здания:

а) размер рабочей зоны: длина 4,5 м, ширина 4,5 м, высота 3 м;

б) остекление помещений: 1 окно размером 2 × 2 м с юго-запада;

в) искусственное освещение - LPO 12-2×40-904 (производство PHILIPS);

г) внутренняя отделка стен - свет;

е) помещение, в зависимости от визуальных условий работы, относится к категории IV (размеры предметов, которые отличаются в работе от 1 до 10 мм и более).

Пространственный план показан на рисунке 1.

Общая площадь номера составляет 20,25 м2. Объем работ составляет 60,75 м3, что обеспечивает необходимый объем работ для трех человек. Это рабочие помещения здания, которые не расположены вблизи железнодорожной линии или загрязненной автомагистрали, аэропорта и т.д., поэтому нет внешних источников шума, влияющих на рабочий процесс - нет. Рабочие помещения не расположены вблизи железнодорожной линии или загрязненной автомагистрали, аэропорта и т.д., поэтому нет внешних источников шума, влияющих на рабочий процесс - нет.

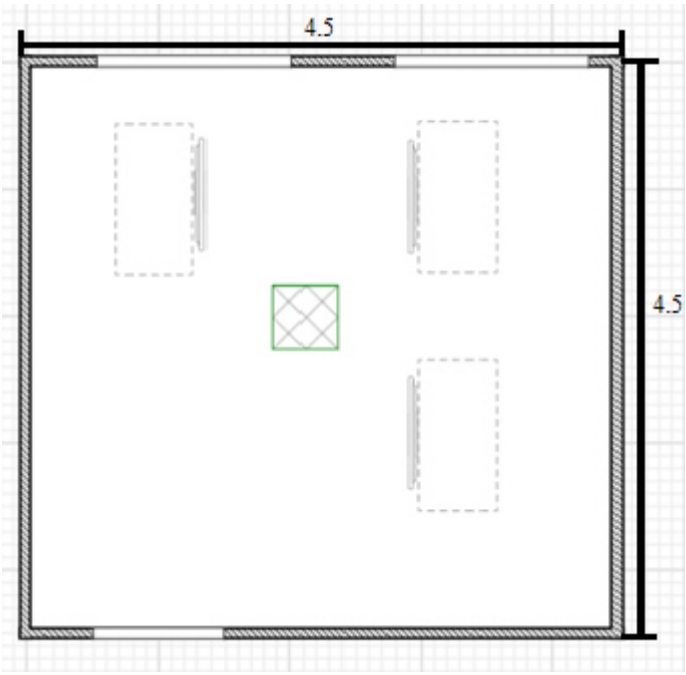


Рисунок 18 - План помещения

Характеристики используемого оборудования. Модель системы создается и запускается на ноутбуке, сборка и сварка пластинчатых элементов в сварочной станции производится в отдельном помещении на стандартном столе. В комнате 3 блокнота:

а) ноутбук HP Pavilion 15-p263ur (IntelCore i7 5500U 2.4Ghz/15.6" /13666x768/6Gb/750Gb/NVIDIA GeForce 840M/DVD-RW/Wi-Fi/Bluetooth/Win8.1);

б) источник питания: переменное напряжение 220-250 В, частота 50-60 Гц, мощность 350 Вт;

в) источник питания: переменное напряжение 220 В, частота 50 Гц, мощность 550 Вт;

г) LPO 12-2×40-904 (производство Samsung);

д) источник питания: переменное напряжение 220 В, частота 50 Гц, мощность 65 Вт, напряжение лампы 103 В.

Это устройство не издает много шума. Ноутбуки вряд ли могут загореться или погибнуть от поражения электрическим током, а установленного огнетушителя достаточно для предотвращения пожара.

Микроклиматические условия. Микроклиматические условия на самом деле настолько приемлемы, что длительное и систематическое воздействие может быстро привести к временным изменениям и стандартизации функционального и теплового состояния организма, а стрессовое функционирование терморегулятора не выходит за пределы физиологической адаптивности.

Решение этой проблемы лежит в следующих областях: пространственное планирование и проектирование зданий, рациональное расположение оборудования, механизация и автоматизация производственных процессов, дистанционное управление и мониторинг, создание эффективных производственных процессов и оборудования, позволяющих обеспечить эффективную теплоизоляцию оборудования, защиту работников от различных типов нагревательных экранов и адекватную вентиляцию, рационализацию работы и отдыха, использование СИЗ (средств индивидуальной защиты).

Здание относится к I классу огнестойкости (СНИП РК 2.02-05-2002) (здания с несущими конструкциями и ограждениями из натуральных или искусственных материалов, бетона или железобетона с использованием негорючих материалов в перекрытиях). Операционная пожарная относится к классу "D". В соответствии со стандартами пожарной безопасности административного здания и отдельных помещений, а также технологического оборудования, они оснащены первичными средствами пожаротушения в соответствии со стандартами.

Природное освещение не обеспечивает полного рабочего дня, необходимого освещения, со временем может измениться или позднее, когда станет темно и естественного освещения будет недостаточно, так что на рабочем месте будет установлена общая система искусственного освещения сжиженных газовых ламп. Климатические условия эксплуатации прибора такие же, как и у персонала.

4.3 Анализ естественной освещенности

Площадь боковых проемов при боковом освещении определяется из следующей формулы:

$$100 * \frac{S_0}{S_n} = \frac{e_N \times K_з \times \eta_0}{\tau_0 \times \tau_1} \times K_{зд}, \quad (1)$$

где S_0- площадь световых проемов при боковом освещении, м2;

S_n – площадь пола помещения, м2;

e_N – нормируемое значение КЕО;

$K_З$ –коэффициент запаса;

η_0– световая характеристика окон;

τ_0– общий коэффициент светопропускания;

r_1– коэффициент, учитывающий повышение КЕО при боковом освещении, благодаря свету, отраженному от поверхности помещения и подстилающего слоя, примыкающего к заданию;

$K_{зд}$– коэффициент, учитывающий затемнение окон противостоящими зданиями.

Определим площадь пола помещения:

$$S_n = L \cdot B, \quad (2)$$

$$S_n = 4{,}5 \cdot 4{,}5 = 20{,}25\ м^2 \quad (3)$$

Нормируемое значение *КЕО,* e_N, для заданий, располагаемых в различных районах определять по формуле:

$$e_N = e_H \cdot m_N \quad (4)$$

где m_N – коэффициент светового климата.

Учитывая заданный световой пояс (г. Алматы), приняв ориентацию световых проемов *З, В* определим:

$$m_N = 0.65$$

e_H – значение КЕО.

Учитывая *Iа* разряд зрительных работ, найдем:

$$e_H = 2.0$$

Следовательно:

$$e_N = 2.0 \cdot 0.65 = 1.3$$

Учитывая тип помещения, найдем коэффициент запаса. $K_з$*=1.2* при *ЕО* вертикально. Для определения световой характеристики, η_0, необходимо рассчитать отношение длины помещения к его глубине $\frac{L}{l}$, отношение ширины помещения к расчетной высоте $\frac{l}{h_{\text{расч}}}$.

$$l = 4{,}5 - 1 = 3{,}5\ м$$

$$\frac{L}{l} = \frac{4{,}5}{3{,}5} = 1{,}28$$

Найдем $h_{расч}$:

$$h_{расч} = h_{0k} + h_{н.ок.} - h_{р.п.}$$

$h_{расч}$*=4,5-0,5-0,8=3,2 м;*

$$\frac{l}{h_{рас}} = \frac{3{,}5}{3{,}2} = 1.09 \approx 1.1$$

$$\frac{l}{B} = \frac{3{,}5}{4{,}5} = 0.77 \approx 1$$

Учитывая найденные отношения примем световую характеристику, $\eta_0 = 8{,}5$.

Общий коэффициент светопропускания, τ_0, рассчитывают по формуле:

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4,$$

где τ_1 – коэффициент светопропускания материала, принимаемый по таблице 4. Так как в качестве светопропускающего материала используется стекло листовое двойное, то:

$$\tau_1 = 0.8$$

τ_2 – коэффициент, учитывающий потери света в переплетах светопроема. Определяется с помощью таблицы 5 с учетом использования стальных двойных глухих переплетов:

$$\tau_2 = 0.8$$

τ_3 – коэффициент, учитывающий потери света несущих конструкциях, при, боковом освещении:

$$\tau_3 = 1$$

τ_4 – коэффициент, учитывающий потери света в солнцезащитных устройствах, принимается по таблице 7. Выбираем убирающиеся регулируемые жалюзи и шторы (межстекольные внутренние, наружные)

$$\tau_4 = 1$$

Следовательно:

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 = 0.8 \cdot 0.8 \cdot 1 \cdot 1 = 0.64$$

$$\rho_{ср} = \frac{\rho_{пот}\rho_{стен}\rho_{пол}}{3}\% = \frac{70 + 50 + 10}{3} \approx 0{,}5$$

r_1=1,7

Учитывая $H_{зд}$=18 и P=10 м (расстояние до рядом стоящего здания), учитываем затемнение окон противостоящими зданиями, $K_{зд}$:

$$\frac{P}{H_{зд}} = \frac{10}{18} = 0.55 => K_{зд} = 1.7$$

Зная значение всех параметров, рассчитываем площадь боковых проемов при естественном освещении по следующей формуле:

$$S_0 = \frac{S_n \cdot e_N \cdot K_з \cdot \eta_0}{100 \cdot \tau_0 \cdot r_1} \cdot K_{зд}$$

$$S_0 = \frac{20{,}25 \cdot 1.3 \cdot 1.1 \cdot 8{,}5 \cdot 1{,}7}{100 \cdot 0.64 \cdot 1{,}7} \approx 3.8\, м^2$$

Таким образом данных расчётов естественное освещение удовлетворяет рассчитанному нормативному значения, но надо произвести расчет

искусственного помещения, так как сотрудники работают в вечерние время тоже.

4.4 Анализ искусственной освещенности

Для расчета искусственного освещения используют один из трех методов: по коэффициенту использования светового потока, точечный и метод удельной мощности.

При расчете общего равномерного освещения основным является метод использования светового потока, создаваемого источником света, и с учетом отражения от стен, потолка, пола.

Расчет освещения начинают с выбора типа светильника, который принимается в зависимости от условий среды и класса помещений по взрыво-пожароопасности.

Разряд зрительной работы I, б, поэтому нормируемая освещенность по таблице Ен= 300 лк (при системе общего освещения).

Сначала нужно рассчитать заданное номинальное значение оно должно быть больше 300.

$$E_\tau = \frac{N*n*ф*\mu}{K*S*z} = \frac{1*1*2850*0{,}45}{1.5*20{,}25*1.1} \approx 38.38 лк \quad (5)$$

Получилась у нас 38.38 < 300 что не удовлетворяет условному значению.

Фактическая освещенность E_τ производственного помещения получилось меньше нормативной освещенности $E_н$, поэтому производим реконструкцию помещения, тем самим увеличивая количество светильников в помещения.

Определение расчетной высоты подвеса:

$$h_{расч} = H_{помещения} - H_{свеса} - H_{р.п.} \quad (6)$$

где $H_{свеса} = 0{,}5$ - высота свеса ламп, м;

$H_{р.п.} = 0{,}8$ - расстояние рабочей поверхности над полом, м;

$H_{помещения} = 3$ - высота помещения, м.

$h_{расч}=3-0{,}5-0{,}8=1{,}7$ *м.*

В практике расчетов значения коэффициентов η находятся из таблиц, связывающих геометрические параметры помещения (индекс помещения) с их оптическими характеристиками.

Индекс помещения определяется по формуле:

$$i = \frac{A*B}{h_{расч}*(A+B)} = \frac{4{,}5*4{,}5}{1{,}7(4{,}5+4{,}5)} = \frac{20{,}25}{12{,}15} = 1{,}66 \quad (7)$$

где A- длина помещения, м;

B - ширина помещения, м;

$h_{\text{расч}}$ - расчетная высота, м.

По таблице 15 для светильника типа TLPL228.2x36 находим $\eta = 0{,}55$. Таким образом, количество светильников равно:

$$N = \frac{\mathrm{E}_{\tau} \cdot \mathrm{K}_{З} \cdot \mathrm{S} \cdot \mathrm{z}}{n\phi \cdot \mu} = \frac{300 \cdot 1.2 \cdot 20{,}25 \cdot 1.1}{1 * 2850 * 0{,}45} \approx 6$$

где $E_н = 300$ *лк* - заданное номинальное освещение.
$S = 20{,}25 м^2$ – площадь помещения.
$z = 1{,}1$- коэффициент неравномерности освещения.
n - количество ламп в светильнике.
ϕ = 2850 лм

$N \approx 6$ *шт.*

Определим необходимое расстояние между светильниками по формуле:

$$L = \lambda * h; \tag{8}$$

где L – расстояние между соседними светильниками;

h – высота подвеса светильника над рабочей поверхностью.

Таким образом, необходимое расстояние между светильниками:

$$L = 0.7 * 1.7 \approx 1{,}2\text{м}$$

Расстояние между рядами светильников:

$$L_b = \lambda * h_{\text{р}} = 1.5 * 0.8 = 1.2\text{м}$$

Расстояние между светильником и стеной:

$$L_{a=} \frac{L_b}{3} + [0{,}3; 0.5] = 0.9м$$

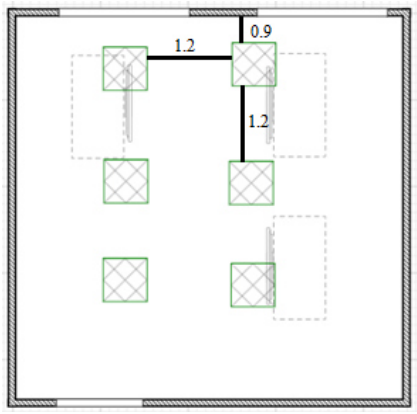


Рисунок 18 – План помещения (после реконструкций)

Описание рабочего места и используемого оборудования. Планировка помещения представлена на рисунке 2.

В рабочем помещении трудятся 3 сотрудника (мужчины – 2, женщины – 1), включая меня, которые имеют служебные места.

Характеристики кабинета: длина *L = 4.5* метров, ширина *W= 4.5* метров, высота H =3 метра. Присутствует окно площадью 4 м^2. Установлен старый кондиционер McQuay.

Характеристики используемого оборудования.

В помещении имеются 2 ноутбука и периферийные устройства:

а) ноутбук HP Pavilion 15-p263ur (Intel Core i7 5500U 2.4Ghz/15.6"/1366x768/6Gb/750Gb/NVIDIA GeForce 840M/DVD-RW/Wi-Fi/Bluetooth/Win8.1);

б) электропитание: переменное напряжение 220-250 В, частотой 50-60 Гц., мощность 350 Вт;

в) принтер HP Laser Jet Pro P1102 (черно-белый / лазерный / настольный /349x196x233 мм);

г) электропитание: переменное напряжение 220 В, частотой 50 Гц., мощность 550 Вт;

Оборудования не представляют шумовую угрозу. Анализ условий труда показал, что слабым местом является вентиляция, в связи с этим в данном разделе производится расчет искусственной вентиляции.

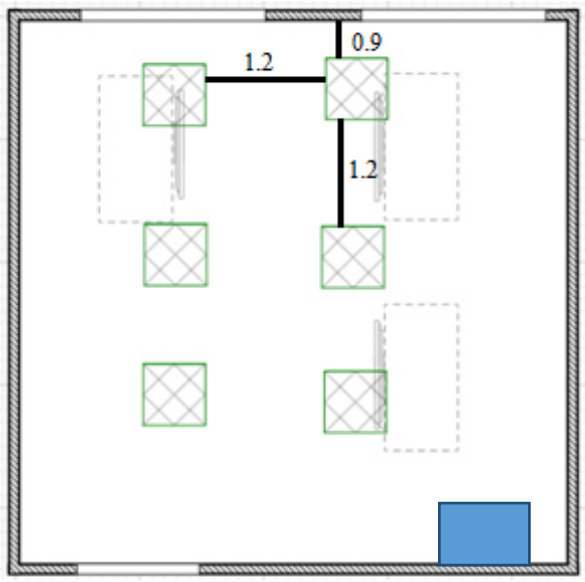


Рисунок 19 – Планировка рабочего помещения

4.5 Расчет тепловых нагрузок в помещении

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние).

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние).

Наружные тепловые нагрузки. В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными. Теплопоступления и теплопотери в результате разности температур определяются по формуле:

$$Q_{огр} = V_{пом} * X_о * (t_{Нрасч} – t_{Врасч}), \text{ Вт (0.1)}, \quad (9)$$

где $V_{пом}$ – объем помещения, м^3;

$V_{пом}$ = 4.5*4.5*3=60.75 м^3;

$X_о$ – удельная тепловая характеристика, Вт/м^3*^{0}С;

$X_о$ = 0,42 Вт/м^3*^{0}С;

$t_{Нрасч}$ – наружная температура (параметр А). Для холодного периода – средняя температура самого холодного месяца в 14 часов, для теплого периода – средней температуре самого жаркого месяца в 14 часов.

$t_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Для теплого времени года:

$$t_{Нрасч} = 29,4\ ^0С,$$
$$t_{Врасч} = 26\ ^0С,$$
$$Q_{огр}= 60,75*0,42·3,4=86,75 \text{ Вт}$$

Для холодного времени года

$$t_{Нрасч} = -9\ ^0С,$$
$$t_{Врасч} = 19\ ^0С,$$
$$Q_{огр} = 60,75·0,42·28 = 714,42 \text{ Вт}.$$

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие. Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле:

$$Q_р= (q^I F^I_о+ q^{II}F^{II}_о) * \beta с.з \ (0.2), \quad (10)$$

где q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, Вт/м^2;

F^I_0, F^{II}_0 – площади светового проема, облучаемые и необлучаемые прямой солнечной радиацией, м^2;

βс.з. – коэффициент теплопропускания. Для штор-жалюзи с металлическими пластинами:

$$\beta с.з. = 0,15$$

При отсутствии наружных затеняющих козырьков, ребер и т. д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^I_0 = F^{II}_0 = F_0 = 0$:

$$Q_p = q^{II} F_0 * \beta с.з = q_{вр} * K^T_1 * K_2 * \beta с.з * n * S_0, \quad (11)$$

где $q_{вп}$; $q_{вр}$ – тепловые потоки от рассеянной радиации, Вт/м^2. Для широты в 44^0 СШ после полудня в 14-15 ч. при расположении ЮВ:

$$q_{вр} = 63 \text{ Вт/м}^2;$$

$F_o = nS_o = 2*2 = 4$ м^2 – площадь светового проема (n – число окон; S_o – площадь 1 окна);

K_1 – коэффициент затемнения остекления переплетами (K^T_1 – для проемов в тени).

$K^T_1 = 1,28$;

K_2 – коэффициент загрязнения остекления:

$K_2 = 0,95$.

Тогда: $Q_p = 63*1,28*0,95*0,15*4 = 45,96$ Вт.

Для широты в 44^{0}СШ после полудня в 14-15 ч. при расположении ЮЗ:

$$q_{вр} = 101 \text{ Вт/м}^2;$$

$$F_o = nS_o = 2*2 = 4 \text{ м}^2$$

Тогда: $Q_р = 101*1,28*0,95*0,15*4 = 73,69$ Вт

Тогда общее теплопоступление солнечного излучения с обеих сторон равно: $Q_р = 45,96+73,69 = 119,65$ Вт

Внутренняя тепловая нагрузка. Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:

- выделяемого людьми;
- выделяемого лампами и осветительными, электробытовыми приборами;
- выделяемого компьютерами, печатающими устройствами;

Летом при 24 ^{0}С один мужчина выделяет явного тепла 67 Вт, а общего – 102 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$$Q^я_л = 67*2 + 67*1*0,85 = 190,95 \text{ Вт}$$

А выделение общего тепла:

$$Q_л^о = 102*2 + 102*1*0,85 = 290,7\ Вт$$

Зимой при 18 ^{0}С один мужчина выделяет явного тепла 89 Вт, а общего – 104 Вт. Тогда выделение явного тепла в помещении составит:

$$Q_з^я = 89*2 + 89*1*0,85 = 253,65\ Вт$$

А выделение общего тепла:

$$Q_з^о = 104*2 + 104*1*0,85 = 296,4\ Вт$$

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле:

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол},\ \ Вт \qquad (12)$$

где η – коэффициент перехода электрической энергии в тепловую (для лампы накаливания $\eta=0,92-0,97$);

$N_{осв}$ – установленная мощность ламп (N=36 Вт);

$F_{пол}$ – площадь пола:

$F_{пол}$ = 4,5*4,5=20,25 м^2

Тогда:

$$Q_{осв} = 0,92*36*20,25 = 670,68$$

Тепло, выделяемое производственным оборудованием, определяется по формуле:

$$Q_{об} = N_{уст} \cdot K \qquad (13)$$

$$Q_{об} = 0,3 * 3 * 0,75 * 10^3 = 0,67\ кВт.$$

Теплопритоки, возникающие за счёт находящейся оргтехники – это 30% мощности оборудования:

$$Q_{орг} = 3 * 0,3 * 0,3 * 10^3 = 0,27\ кВт$$

Расчет теплового баланса помещения. На основании выполненных расчетов составим баланс теплопоступлений в помещении:

$$Q_{изб} = Q_р + Q^я + Q_{осв} + Q_{об} + Q_{орг} + Q_{огр}$$

лето: $Q_{изб}^Л = 119,65 + 190,95 + 670,68 + 670 + 270 + 86,75 = 2,1\ кВт$

зима: $Q_{изб}^З = 119,65 + 253,65 + 670,68 + 670 + 270 + 714,42 = 2,7\ кВт$

Так как тепловой баланс для лета больше зимнего теплового баланса, то рассчитаем теплонапряженность воздуха по формуле:

$$Q_н = \frac{Q_{изб.лето} \times 860}{V_{пом}} \qquad (14)$$

$$Q_н = \frac{2{,}1 \cdot 860}{60.75} = 29{,}73\ ккал/м3$$

при $Q_н$ >20ккал/м^3, Δt =8 °С,

при $Q_н$ <20ккал/м^3, Δt =6 °С.

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} \times 860}{C \times \Delta t \times \gamma}$$

$$L = \frac{0{,}27 \cdot 860}{0{,}21 \cdot 8 \cdot 1{,}206} = 114{,}60\ м3/час$$

где *C=0,21 ккал/(кг · °C)* – теплоемкость воздуха,

γ=1,206 кг/м^3 – удельная масса приточного воздуха.

4.6 Выбор кондиционера и схема расположения

Исходя из полученных результатов, для удаления лишнего тепла и очистки воздуха нужно использовать вентиляционную систему, которая способна обеспечить требуемую подачу воздуха L=114,60 (м3/ч). В данном случае подойдет Кондиционер MIDEA MDSA-09HRFN1 INVERTER. Данный кондиционер способен обеспечить подачу воздуха до 1200 м3 /ч.

Технические характеристики:

- мощность (охлаждение): 2.93 кВт;
- мощность (обогрев): 2.93 кВт;
- потребляемая мощность при охлаждении: 2200 Вт;
- потребляемая мощность при обогреве: 2240 Вт;
- обслуживаемая площадь: 28 м2;
- уровень шума внутреннего блока: 37-41 дБ;
- уровень шума внешнего блока: 48 дБ;
- цвет: серый.

Характеристики подключения:

- вентиляция: 1200 м3/час;
- класс энергоэффективности при охлаждение/обогреве: А++/А+;
- электропитание, В/Гц/Ф:220 Вт;
- энергопотребление в режиме ожидания не более 1 Вт.

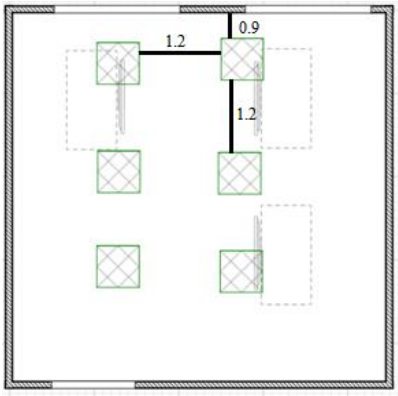


Рисунок 20 – Расположение кондиционера в помещении

Вывод по четвертой главе. В этом разделе моего дипломного проекта я рассмотрел и рассчитал анализ естественной освещённости, анализ искусственной освещённости. Для данного помещения использовался светильник ЛПО 12-2×40-904 с недостаточным количеством света при ночной работе, и мне пришлось заменить этот светильник на новые светильники типа TLPL228.2x36. Так же я рассмотрел и рассчитал воздушные показатели для благоприятных условий труда, а именно, тепловые нагрузки в помещении, наружные и внутренние. По расчетам, для создания хороших условий труда необходим один кондиционер с подачей воздуха не менее 114,60 м3 /ч, в моем случае используется кондиционер MIDEA AURORA 1 MSAB-24HRN1-WG с подачей воздуха до 1200 м3 /ч.

5 Технико-экономическое обоснование

Модель, проектирование в рамках дипломной работы, предназначен для систем информационной защиты предприятия, видео/аудио контроля, мониторинга и анализа деятельности сотрудников. Умная система мониторинга и контроля сотрудников обеспечивает полный контроль компьютеров, предотвращает от утечки конфиденциальной информации на предприятии.

5.1 Расчет трудоемкости разработки программного комплекса

Приведен перечень основных этапов и работ, которые нужно выполнить для определения трудоемкости разработки программного обеспечения. Трудоемкость работы определялась согласно нормам времени на проведение расчетов, анализа и исследований. Форма распределения работ по этапам с указанием трудоемкости их выполнения приведена в таблице 4.

Таблица 4 - Распределение работ по этапам и оценка их трудоемкости

Этапы разработки ПО	Вид работы	Трудоемкость, чел. час.
Этап 1	Формирование задач	18
Этап 2	Разработка и утверждение ТЗ на проектирование программно-аппаратного комплекса	21
Этап 3	Исследование и поиск подобных программ и устройств	18
Этап 4	Исследование и поиск соответствующей литературы	14
Этап 5	Выбор среды разработки программного обеспечения	20
Этап 6	Реализация проекта	13
Этап 7	Отладка программного обеспечения	32

Продолжение таблицы 4

Этап 8	Оформление отчета и выводов	16
Этап 9	Тестирование проекта	15
Этап 10	Разработка ПО для материнской платы	23
Этап 11	Разработка внешнего виде: выбор корпуса и установка материнской платы для сервера	26
Итого: трудоемкость выполнения дипломного проекта		216

Длительность рабочего дня равна 8 часам. Тем самым количество затраченных дней на распределение работ по этапам и оценка их трудоемкости равна 27 рабочих дней. 216:8=27/

5.2 Расчет расходов на разработку программного комплекса

Расчет расходов на разработку программного комплекса выполняется на базе имеющейся сметы, которая состоит следующих статьей:

– расходы на материальные ресурсы;

– расходы на оплату труда;

– социальный налог;

– амортизация основных фондов.

Статья «Материальные расходы» состоит из основных и вспомогательных материалов, энергии, которые необходимы для разработки аппаратного комплекса. Расчет расходов на материальные ресурсы производится по форме, приведенной в таблице 5.

Таблица 5 – Расходы на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Офисная бумага, А4	International Paper	Упаковка	2	1500	3000
Тетрадь (96 листов)	Natural	Штук	1	250	250
Блокнот (96 листов)	OFFICE	Штук	1	650	650
Ручка	Maxriter	Штук	5	120	600
Карандаш	Koh-i-noor	Штук	5	65	325
Мышь, клавиатура и коврик	HP	Штук	3	7990	7990
Итого					12815

Для проектирование программно-аппаратного комплекса будет использоваться ноутбук, операционная система, программное обеспечения, материнская плата и корпус для неё.

Таблица 6 – Расходы для проектирование программно-аппаратного комплекса

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	HP 15-bs564ur	Шт.	1	190000	190000
Сервер	Dell PowerEdge T110 II	Шт.	1	48900	48900
Модем	TP-Link	Шт.	1	8500	8500
Итого					247400

Общая сумма расходов на материальные ресурсы ($З_м$) определяется по формуле:

$$З_м = \sum P_i \times Ц_i, \quad (5.1)$$

где P_i– расход i-го вида материального ресурса, натуральные единицы;

$Ц_i$– цена за единицу i-го вида материального ресурса, тг;

i – вид материального ресурса;

n – количество видов материальных ресурсов.

$З_м = 12815 + 247400 = 260\ 215$ (тг)

Общие затраты для реализации программно-аппаратного комплекса составляют: 260 215 тенге.

5.3 Расчет расходов на электроэнергию

Важно рассчитать расходы на электроэнергию, потому что в процессе работы используется электрооборудование. Время работы оборудования для проектирование программно-аппаратного комплекса берется равным 224 часов для ноутбука, данное количество часов было рассчитано в таблице 5.1. Для материнской платы время работы для проектирование программно-аппаратного комплекса берется равным 12 часов, так нет необходимости постоянного его использования.

$$Э = З_{эл.эн.обор} + З_{доп.нуж}, \quad (5.2)$$

где $З_{эл.эн.обор}$ – расходы на электроэнергию оборудования;

$З_{доп.нуж.}$ – расходы электроэнергии на дополнительные нужды.

Расходы электроэнергии на оборудование рассчитывается по формуле:

$$З_{эл.эн.обор} = \sum W \times К_{исп} \times S \times T, \quad (5.3)$$

где W – потребляемая мощность, Вт;

$К_{исп}$ – коэффициент использования ($К_{исп}$ = 0,7..0,9);

T – время работы;

S – тариф (1кВт/ч = 18,32тг).

Сводные результаты расчета затрат на электроэнергию представлены в таблице 7.

Таблица 7 – Расходы на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/ кВтч	Сумма, тг
Ноутбук	0,6	0,7	216	18,32	1661,9
Сервер	0,08	0,9	100	18,32	131,9
Модем	0,5	0,9	12	18,32	98,9
Кондиционер	0,8	0,9	200	18,32	2638,08
Освещение	0,3	0,7	216	18,32	830,9
Итого					5361,7

$З_{эл.эн.обор}$= 1661,9+131,9+98,9+2638,08+830,9=5361,7(тенге)

Расходы на дополнительные потребности берутся по укрупненному показателю в размере 5% от затрат на оборудование:

$$З_{доп.нуж} = 5\% \times З_{эл.эн.обор} \quad (5.4)$$

Расходы на дополнительные потребности рассчитаны по формуле (5.4):

$З_{доп.нуж} = 0,05 \times 5361,7 = 268,08$ (тенге)

Таким образом суммарные расходов на электроэнергию составляют:

$Э = 5361,7 + 268,08 = 5629,78$(тенге)

5.4 Расчет расходов на оплату труда

Над разработкой программно-аппаратного комплекса работают два сотрудника:

- руководитель проекта – он изучает предметную область, проводит анализ требований к системе, занимается внедрением и поддержкой;
- помощник руководителя проекта – поддержкой при проектировании модели, занимается вспомогательными действиями.

Общая сумма затрат на оплату труда ($З_{тр}$) определяется по формуле:

$$З_{тр} = \sum ЧС_i \times Т_i \quad (5.5)$$

где $ЧС_i$ – часовая ставка i-го работника, тг;

Ti – трудоемкость разработки модели, чел.×ч;

i – категория работника;

n – количество работников, занятых разработкой ПП.

На этапах разработки, участники разработки задействованы неравноценно, для этого необходимо рассчитать часовую ставку помощник руководителя, а затем общий размер заработной платы.

Часовая ставка помощник руководителя может быть рассчитана по формуле:

$$ЧС_i = \frac{ЗПi}{ФРВi} \quad (5.6)$$

где *Зпі* – месячная заработная плата і-го работника, тг;

ФРВі - месячный фонд рабочего времени і-го работника, час;

Месячная заработная плата сотрудников:

- руководитель проекта – 180 000 тг;
- помощник руководителя – 120 000 тг;
- рабочие часы в день составляют 8 часов.

Рабочих дней в месяц составляют 22 дня после вычета выходных 2 дней.

$$ЧС_i = 180\,000 / 22 \times 8 = 1\,022{,}72 \text{ тг/ч}$$
$$ЧС_i = 120\,000 / 22 \times 8 = 681{,}81 \text{ тг/ч}$$

Часовая ставка научного руководителя составляет 1 022,72 (тг/ч), трудоемкость разработки – 90 часов из таблицы 5.1 путем складывания этапов разработки 2 = 15, 5 = 20, 10 = 23, 11 = 26. Часовая ставка разработчика составляет 681,81 (тг/ч), трудоемкость разработки из таблицы 5.1 – 216 ч.

Рассчитаем общую сумму расходов на оплату труда по формуле (5.5):

$$З_{тр} = 1\,022{,}72 \times 90 + 681{,}81 \times 216 = 239\,315{,}76 \text{ (тенге)}$$

Сводные результаты расчета расходов на оплату труда показаны в таблице 8.

Таблица 8 – Расчёт основной заработной платы разработчиков.

Категория работника	Квалификация	Трудоемкость разработки ПП, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель проекта	Инженер-программист	90	1 022,72	92 044,8
Разработчик	Программист	216	681,81	147270,96
Итого				239 315,76

5.5 Расчет расходов по социальному налогу

Социальный налог – согласно Налоговому кодексу Республики Казахстан составляет 9,5 % от ФОТ (фонда оплаты труда). Следует отметить, что пенсионные отчисления не облагаются социальным налогом.

$$C_н = (ФОТ - ПО) \times 0{,}095 \quad (5.7)$$

где *ПО* - отчисления в пенсионный фонд, 10% от ФОТ.

Социальный налог рассчитываем по формуле (5.7):

$$ПО = 239\,315{,}76 \times 0{,}1 = 23\,931{,}576 \text{ тенге;}$$

$$C_н = (239\,315{,}76 - 23\,931{,}576) \times 0{,}095 = 20\,461{,}49 \text{ тенге}$$

Сводные результаты расчета расходов представлены в таблице 5.7.

Таблица 9 - Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель проекта	1	92 044,8	9 204,48	7 869,75
Разработчик	1	147270,96	14 727,09	12591,66
Итого				20 461,49

5.6 Амортизация основных фондов и прочие расходы

Годовые нормы амортизации ОФ принимаются по налоговому кодексу РК или определяются, исходя из возможного срока полезного использования ОФ. Амортизация основных фондов определяется:

$$А_г = \frac{С_{об} \times Н_а}{100} \quad (5.8)$$

где $C_{об}$ – стоимость оборудования;

H_a – норма амортизации (норма амортизация = 20);

По формуле 5.8 рассчитаем сумму амортизационных отчислений за год для ноутбука:

$$А_г = \frac{190000 \times 20}{100} = 38\,000 \text{ тг}$$

Рассчитаем сумму амортизации за время разработки:

$Н_а$ – норма амортизации (норма амортизация = 27);

216 часов трудоемкость выполнения дипломного проекта, 8 длительность рабочих часов для одного дня берутся из таблицы 5.1

$$\frac{216}{8} = 27$$

$$А_р = \frac{38\,000 \times 27}{365} = 2\,811 \text{ тг}$$

Аналогичным способом рассчитаем сумму амортизации для остального оборудования.

Результаты расчетов приведены в таблице 5.6

Таблица 10 - Амортизация основных фондов

Наименование оборудования	Стоимость оборудования, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Ноутбук	190 000	20	38 000	2 811
Сервер	48500	20	9700	744,1
Модем	8900	15	1355	102,4
ИТОГО амортизация основных средств			49055	3657,5

Смета затрат на разработку программного продукта. На основании полученных данных по отдельным статьям составляется смета затрат на разработку программного продукта по форме, приведенной в таблице.

Таблица 11 – Смета расходов на разработку программного продукта

Статьи расходов	Сумма, тг	Проценты %
Расходы на оборудование и материальные расходы	260215	54 %
Расходы на оплату труда	239 315,76	37 %
Социальные налоги	20 461,49	4 %
Расходы на электроэнергию	5629,79	1 %
Амортизация основных фондов	3657,5	0 %
Прочие расходы (интернет)	9589	
Итого по смете	538 868,54	

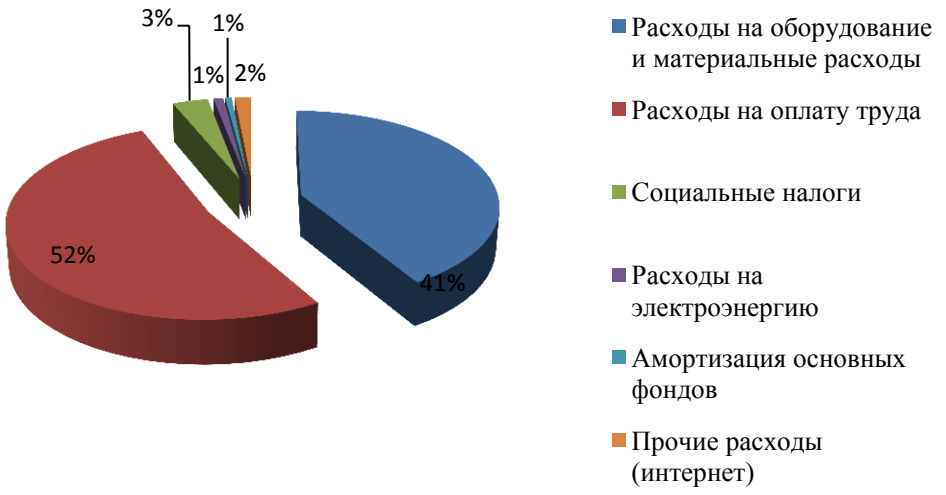


Рисунок 22 - Диаграмма структуры затрат

5.7 Определение возможной (договорной) цены программного продукта

Величина возможной (договорной) цены программного продукта устанавливается на основе эффективности, качества и сроков её выполнения на уровне, отвечающем экономическим интересам заказчика (потребителя) и исполнителя.

Договорная цена ЦД для прикладных программных продуктов рассчитывается по формуле:

$$Ц_Д = З_{НИР}(1 + \frac{Р}{100}) \quad (5.9)$$

где $З_{НИР}$ - расходы на разработку ПП, тг;

$Р$ – средний уровень рентабельности ПП, % (принимается в размере 20%).

$$Ц_Д = 538\,868{,}54 \times (1 + 20/100) = 538\,868{,}54 + 107\,773{,}70 = 646\,642{,}24 \text{ тенге}$$

Далее определяется цена реализации с учетом налога на добавленную стоимость (НДС), ставка (НДС) устанавливается законодательно. Налоговым Кодексом РК. На 2017 год ставка НДС установлена в размере 12%.

Цена реализации с учетом НДС рассчитывается по формуле:

$$Ц_р = Ц_Д + Ц_Д \times НДС \quad (5.10)$$

$$646\,642{,}24 + 646\,642{,}24 \times 0{,}12 = 647\,287{,}14 + 77\,597{,}07 = = 724\,884{,}21 \text{ тенге.}$$

Себестоимость = 538 868,54 тенге из таблицы 5.9

Прибыль = 107 773,70 тенге

Цена реализации с учетом НДС = 724 884,21 тенге

Вывод по пятой главе. В данной главе дипломной работы мною были рассчитаны экономические расходы, которые нужны для проектирование программно-аппаратного комплекса. Расходы состоят из:

- расходов трудоемкости проектировании программно-аппаратного комплекса;
- расходы на разработку программно-аппаратного комплекса;
- расходы на электроэнергию;
- расходы на оплату труда;
- расходы по социальному налогу;
- амортизация основных фондов и прочие расходы.

Договорная цена программно-аппаратного комплекса будет равна 724 884,21 тенге. Смета расходов на проектирование программно-аппаратного комплекса будет равна 538 868,54 тенге. Прибыль (рентабельность) будет равна 107 773,70 тенге.

Заключение

Современная производственная компания характеризуется информационной системой с присущими ей процессами сбора, обработки, хранения и накопления информации. Эти процессы используют информацию с различных уровней доступа и функциональных приложений, которые могут подвергаться различным типам угроз. И сейчас, в связи с активным развитием информационных технологий в сфере промышленных предприятий, растет число проблем, связанных с информационной безопасностью.

В работе проводится анализ и теоретическое обобщение методов, средств и технологий, известных для защиты конфиденциальной информации, применительно к промышленной компании ТОО "ПК4U".

В соответствии с Законом Республики Казахстан "Об информатизации", Законом Республики Казахстан "О персональных данных и их защите" необходимо принять меры по защите персональных данных от раскрытия, использовать меры по защите электронных информационных ресурсов и систем контроля доступа и регистрации доступа к информации. В результате в качестве оптимального метода защиты информации в условиях решения задач IB предприятия была выбрана система DLP на базе решения "Инспектор" аппаратного и программного обеспечения.

АПК "Инспектор" является национальным продуктом и эффективным методом защиты информационных ресурсов и информационного общества в целом. Эта система предлагает:

- целостность данных;
- значительно снижают риск утечки ценной информации;
- возможность предотвращения потери конфиденциальной информации;
- снизить риски, связанные с пренебрежением и неграмотностью пользователей компьютеров;
- интегрирование с устройствами сторонних производителей;
- повышение производительности труда сотрудников.

Все задания выполняются при написании диссертации:

- проведен систематический анализ уязвимости системы информационной безопасности современного предприятия;
- рассмотрена общая структура информационной системы производственной безопасности;
- были выявлены потенциальные источники угроз и уязвимости;
- исследуется и проводится сравнительный анализ современных методов и систем защиты информации;
- обосновано внедрение нового метода защиты ИС;
- в ТОО «PC4U» внедрен АПК «Инспектор»;
- приведены конкретные предложения и рекомендации по защите ИС ТОО «PC4U»;

В дипломной работе проанализирована актуальная проблема защиты от потери конфиденциальной информации и ограниченного доступа к ней в

информационной среде ТОО «PC4U», что требует внедрения новых программно-технических решений. Приведены необходимые статистические данные и параметры, основные функции "инспектора", последовательность и методы установки и адаптации аппаратного и программного обеспечения.

Выявлены характеристики DLP-технологии как основного инструмента защиты от потери данных, методы установки клиентской (агентской) части сельскохозяйственного и промышленного комплекса на ПК: вручную, с помощью программного обеспечения ActiveDirectory. Работа содержит структурную и функциональную схему АПК "Инспектор", основной алгоритм его работы и необходимые результаты анализа эффективности системы, полученные после ее внедрения в опытно-промышленном режиме на основе экспериментальных отчетов.

На экспериментальной основе проведена оценка эффективности поддержки СИ с использованием аппаратно-программного решения на базе ТОО «PC4U» и определение степени коррекции реакции системы на нарушения требований СИ. Анализ нарушений правил охраны труда проведен на 15 рабочих местах.

В результате анализа информационной системы ТОО «PC4U» было выявлено несколько нарушений в работе сотрудников с ПК, рабочими файлами и документами, программами и другими интернет-ресурсами. После выявления нарушений через систему контроля и надзора за действиями "инспектора" были предприняты определенные меры.

Повторный анализ с интервалом в 15 рабочих дней показал прямое увеличение результатов работы и качества распределения рабочего времени. Сотрудники компании начали эффективно использовать свое рабочее время и брать на себя ответственность. Количество посещений социальных сетей и других интернет-ресурсов сократилось на 87 процентов.

В ходе подготовки работы был также проведен анализ слабых сторон официального сайта ТОО «PC4U»http://pc4u.kz/.

В результате анализа были выявлены следующие недостатки:

- тестирование на проникновение показало возможность использования ошибок и программного кода для использования вредоносного кода или несанкционированного доступа;

- при проверке на постоянство авторизации выявляется отсутствие защиты от повторного ввода пароля и возможность его восстановления, скорость восстановления пароля учетной записи достаточно высока;

- отсутствие соединение уровня защищенных сокетов (SSL)соединения;

- сайт уязвим для атак на языке структурированных (SQL).

На основании полученных результатов разработана концепция информационной безопасности, включающая рекомендации по минимизации количества рисков и уязвимостей и повышению эффективности защиты ТОО "PC4U".

Система была оптимально адаптирована под производственную компанию ТОО "PC4U". Внедрение АПК "Инспектор" позволяет строить,

анализировать и оценивать информационные ресурсы информационной безопасности информации, данных, файлов, определять степень утраты важной информации третьими лицами.

В рамках данной дипломной работы начат опытно-промышленный режим работы агропромышленного комплекса "Инспектор", эта система будет продолжать функционировать. Будут созданы другие глобальные конфигурации и подготовлены все необходимые документы. С помощью этой системы, которая оценивает все информационные потоки, пока люди работают с документами и файлами, можно классифицировать все данные в соответствии со степенью конфиденциальности и вносить изменения в программу: Создавайте папки, делайте дополнительные настройки, создавайте более удобный интерфейс.

Таким образом, внедрение системы АПК "Инспектор" позволяет решить проблему блокирования утечки ограниченной информации по каналам связи в инфраструктуре ТОО "PC4U". Возможности системы также позволили определить структурную часть - источник и канал утечки, что в дальнейшем исключает любые попытки утечки и хищения информационных ресурсов. Из этого можно сделать вывод, что выбор и внедрение в информационную систему (в нашем случае в промышленную компанию) решения "Инспектор" аппаратного и программного обеспечения позволит принять решение по проблемам СИ на достаточно эффективном уровне.

Внедрение в ТОО "PC4U" агропромышленного комплекса "Инспектор" (DLP System) является реальной и экономически обоснованной задачей. Возмещение затрат на внедрение "Инспектора" осуществляется за счет повышения уровня трудовой дисциплины персонала, оптимизации системы защиты информационной среды и повышения эффективности работы руководителей структурных подразделений.

Список использованной литературы

1 Будников А.И. Информационная безопасность и защита информации. 2014 год.

2 Баранова Е.К. Методики анализа и оценки рисков информационной безопасности. Статья. УДК 519.876.5 2015 г.

3 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 24.11.2015 г.)

4 Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности

5 СТ РК 1699-2007. Системы контроля и управления доступом.

6 Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. – М.: Гелиос АРВ, 2005 г. – 224 с.

7 Мазуров В.А., Головин А.В., Поляков В.В. Информационная безопасность: основы правовой и технической защиты информации. Барнаул: Изд-во Алт. ун-та, 2005 г.

8 Корниенко А.А., Слюсаренко И.М. Системы и методы обнаружения вторжений:современное состояние и направления совершенствования ПГУПС,«InfoSoftCom» 2009 г.

9 Макаренко С.И. Информационная безопасность. Учебное пособие. Ставрополь 2009 г.

10 Шубинский М.И. ст. Информационная безопасность. Статья, 2013 г.

11 Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам – Учебное пособие – М.: Горячая линия - Телеком, 2011. – с. 220.

12Березюк Л.П. Организационное обеспечение информационной безопасности: учеб. пособие/Л.П. Березюк. – Хабаровск: Изд-во ДВГУПС,2008. – 188 с.

13 Адрес сайта:http://www.securitylab.ru/blog/personal/aguryanov/30011.php

14 КубеевЕ.К., Каргин С.Т. Учебный процесс в КарГУ. - Караганда: Изд-во КарГУ, 2003. – 9 с.

15 Павленко И.В. «Место информатизации в стратегии формирования инновационного университета» 2015 г.

16 Гмарь Д.В., Крюков В.В., Майоров В.В., Шахгельдян К.И. Единая система регистрации и управления доступом к информационным ресурсам вуза. Труды всероссийской научной конференции «Научный сервис в сети Интернет , Новороссийск», 2003, с. 135-138.

17 Свиряева М.А., Молоткова Н.В., Анкудимова И.А. Организация информационно- образовательной среды вуза на основе технологий дистанционного обучения//Вопросы современной науки и практики. 2010. №

4–6

18 Лукацкий А. Обеспечение информационной безопасности современного предприятия. Статья. 2010 г.

19 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

20 Гагарина Д.А., Хеннер Е.К. Структура высокоразвитой информационно-образовательной среды инновационного университета. 2009 г.

21 Крюков В. В., Майоров В. С., Шахгельдян К. И. Реализация корпоративной вычислительной сети вуза на базе технологии ActiveDirectory // Тр. Всерос. науч. конф. «Научный сервис в сети Интернет». Новороссийск, 2002. – С. 253–255.

22 Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

23 Адрес сайта:http://www.infosec.ru/news/experts/9904

24 Проталинский О.М., Ажмухамедов И. М. Информационная безопасность вуза, Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ., 2009, номер 1, 18–23.

25 Немиткин В. В. Анализ и управление рисками в области защиты информации Диссертационная работа. 2009 г. http://www.dissercat.com/content/analiz-i-upravlenie-riskami-v-oblasti-zashchity-informatsii

26Адрес сайта:http://windata.ru/windows-xp/faq-xp/kratkoe-opisanie-active-directory

27Адрес сайта:http://www.victoria.lviv.ua/html/informatika/lecture10.htm

28Адрес сайта:http://compress.ru/article.aspx?id=20549

29Адрес сайта:http://insp.kz/features/

30Адрес сайта:http://insp.kz/tech/

Аббревиатуры

ARP – AddressResolutionProtocol, Протокол разрешения адресов

BGP – BorderGatewayProtocol, Протокол граничных шлюзов

DNS – DomainNameSystem, Доменная система имен

DoS – DenialofService, Отказ в обслуживании

FTP FileTransferProtocol, Протокол передачи файлов

HTTP – HypertextTransferProtocol, Протокол передачи гипертекстовой информации

IP – Internet Protocol, Межсетевойпротокол

IT – Information technology, Информационныетехнологии

MAC – MediaAccessControl, Управление доступом к среде передачи

NAT – Network Address Translation, Трансляциясетевыхадресов

OSI – Open System Interconnection, Взаимодействиеоткрытыхсистем

SSL – Secure Sockets Layer, Уровеньбезопасныхсоединений

SSH – Secure Shell, Безопаснаяоболочка

TCP – Transmission Control Protocol, Протоколуправленияпередачей

UDP – UserDatagramProtocol, Пользовательский датаграмный протокол

URL – UniformResourceLocator, Унифицированный определитель местонахождения

VoIP – VoiceoverIP, Передача голоса по интернет-протоколу

VPN – VirtualPrivateNetwork, Виртуальные частные сети

VLAN –VirtualLocalAreaNetwork, Виртуальная локальная вычислительная сеть

WWW – WorldWideWeb, Распределенная всемирная сеть

IDS – IntrusionDetectionSystem,Система обнаружения вторжений

СОВ – Система обнаружения вторжений

DMZ – DemilitarizedZone, Демилитаризованнаязона

IP – Internet Protocol

DSL –DigitalSubscriberLine, Цифроваяабонентскаялиния

ISDN– Integrated Services Digital Network, Цифроваясетьсинтеграциейслужб

AD – Active Directory

SMTP– Simple Mail Transfer Protocol, Простойпротоколпередачипочты

IM–Instantmessaging,Система обмена мгновенными сообщениями

USB–UniversalSerialBus, Универсальная последовательная шина

COM – ComponentObjectModel, Объектная модель компонентов

LPT– LinePrintTerminal, Параллельный порт, порт принтера

IMAP– *InternetMessageAccessProtocol*, Протокол прикладного уровня для доступа к электронной почте

POP –*PostOfficeProtocol*, Протокол почтового отделения

GC – GlobalCatalogue, Глобальный каталог

HIPS–Host-basedIntrusionPreventionSystem, системапредотвращениявторжений

АПК – Аппаратно-программный комплекс
ИБ – Информационная безопасность
ИС – Информационная система
ИКТ – Информационно-телекоммуникационные технологии
ППС – Профессорско-преподавательский состав
ЦОР – Цифровые образовательные ресурсы
ПК – Персональный компьютер
АС – Автоматизированная система
ВС – Виртуальное соединение
ВОС – Взаимодействие открытых систем
ЗИ – Защита информации
ИБ – Информационная безопасность
ИВС – Информационное виртуальное соединение
МБ – Монитор безопасности
КС – Компьютерная сеть
МЭ – Межсетевой экран
НСД – Несанкционированный доступ
ПБ – Политика безопасности
РД – Разграничение доступа
СМО – Система массового обслуживания
ТВС – Технологическое виртуальное соединение
ТМО –Теория массового обслуживания
Обозначения и сокращения
АРМ – Автоматизированное рабочее место
ВИ – Видовая информация
ВТСС – Вспомогательные технические средства и системы
ИСПДн – Информационная система персональных данных
КЗ – Контролируемая зона
МЭ – Межсетевой экран
НСД – Несанкционированный доступ
ОБПДн – Обеспечение безопасности персональных данных
ОС – Операционная система
ПДн – Персональные данные
ПМВ – Программно-математическое воздействие
ПО – Программное обеспечение
РИ – Речевая информация
СВТ – Средство вычислительной техники
СЗИ – Средство защиты информации
СПИ – Стеганографическое преобразование информации
СЭУПИ – Специальные электронные устройства перехвата информации
ТКУИ – Технический канал утечки информации
ТСОИ – Технические средства обработки информации
УБПДн – Угрозы безопасности персональных данных
ПИБ – Политика информационной безопасности

ПК – Персональный компьютер

СХД – Сети хранения данных

СКДК – Система централизованного контроля действий, производимых на компьютерах

ПО – Программное обеспечение

Глоссарий

VPN-клиент– программный или аппаратный комплекс, работающий на основе персонального компьютера. Его сетевое ПО изменяется для реализации шифрования и аутентификации трафика.

VPN-сервер– программный или аппаратный комплекс, реализующий функции сервера. Он реализует защиту серверов от несанкционированного доступа из других сетей, а также организацию виртуальной сети между клиентами, серверами и шлюзами.

Шлюз безопасности VPN– сетевое устройство, подключаемое к 2 сетям и реализует функции аутентификации и шифрования для множества хостов, находящихся за ним.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Идентификация – процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими

средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.