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: Организация информационной безопасности предприятия
Специальность: Системы информационной безопасности
Выполнил: Бисентаев Дархан Каирханович Группа СИБ-15-2
Научный руководитель: Покусов Виктор Владимирович

Консультант:
по экономической части:
к.э.н., профессор Ермекбаева Ж.Г.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)

по безопасности жизнедеятельности:
д.т.н., ст. преп. Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О)
_____ «22» Мая 2019 г.
(подпись)

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

Нормоконтролер:
м.т.н., ст. преподаватель Аскарова Н.П.
(ученая степень, звание, Ф.И.О)
_____ «28» 05 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 «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Бисентаеву Дархану Каирхановичу

Тема проекта: Организация информационной безопасности предприятия

Утверждена приказом по университету №_124_ от «_26_» октября 2019 г.

Срок сдачи законченного проекта «_____» _____2019 г.

Целью дипломной работы является изучение общей структуры предприятия, определение потенциальных источников угроз и дальнейшее внедрение оптимального метода защиты информационной системы.

Для достижения указанной цели необходимо решить следующий комплекс задач:

- сбор информации по теме дипломной работы;
- изучение общей структуры информационной системы;
- определение потенциальных источников угроз и уязвимые места;
- изучение и сравнительный анализ современных методов и систем защиты информации;
- внедрение оптимального метода защиты информации для ТОО «PC4U».

Перечень вопросов, подлежащих внедрению в дипломном проекте или краткое содержание дипломного проекта: дипломный проект включает в себя 4 глав, разделенные на подглавы, каждая из которых освещает определенную тематику, используемую при организации информационной безопасности.

В первой главе дипломного проекта представлена общая информация про системный анализ информационной безопасности современного предприятия, а также про их возможные уязвимости и угроз.

Во второй главе дипломного проекта представлен анализ и обоснование оптимального метода защиты информаций.

В третей главе приводится технико-экономическое обоснование проекта.

В четвертой главе рассматриваются необходимые условия для удобной работы сотрудников организаций соответствующим общепринятым положениям.

Основная рекомендуемая литература:

1 А.В., Иванников А.Д., Усков В.Л. Educational Technology & Society 11(1) Технологии обеспечения информационной безопасности корпоративных образовательных сетей 'Государственный научно-исследовательский институт информационных технологий и телекоммуникаций «Информика», Москва. ISSN 1436-4522,2008 г.

2 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.

3 Волков А.В. Обеспечение ИБ в вузе. Журнал "Information Security/ Информационная безопасность" 2006 г. - № 3, 4.

4 Шемяков А.О. Научно-методический аппарат оценки уязвимости системы обеспечения безопасности информации в современном вузе. - Серпухов, 2013.- 130 с.: ил. РГБ ОД, 61 13-5/2197.

Конструкции по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Вычисл. техника	Покусов В.В.	18.05 - 28.05	
Безопасн. исследов.	Бекбасаров Ш.Ш.	05.03-23.05	
Экономика	Трембаева Ис.Г.	04.03 - 22.05	
Нормоконтроль	Аскарова Ж.Б.	18.05 - 28.05	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Системный анализ ИБ совр. пред.	01.02.2019 - 15.02.2019	
Роль информатизации раб. проц.	15.02.2019 - 01.03.2019	
Общая структура ИС пред. ТОО «Эсси»	01.03.2019 - 12.03.2019	
Комплексное обеспечение ИБ	12.03.2019 - 30.03.2019	
Анализ и обоснование опт. методов	30.03.2019 - 12.04.2019	
Выбор и обоснование внедрений	12.04.2019 - 25.04.2019	
Тех. спецификация системы	25.04.2019 - 01.05.2019	
Аппаратно-программный комплекс ТПР	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 _____ (Бисенгаев Д.К.)
(Подпись) (Ф.И.О)

АННОТАЦИЯ

В данной дипломной работе было описано анализ информационной среды, обоснование и внедрение системы защиты АПК «Инспектор» в информационную среду ТОО «PC4U».

В процессе была проанализирована актуальная проблема защиты от утечки информации конфиденциального характера и ограниченного доступа в информационную среду организаций, что требует внедрения новых программно-технических решений.

В разделе «Экономика» были рассчитаны затраты при построении и внедрении системы.

В разделе «Безопасность жизнедеятельности» был произведен рассчет условия труда с соответствующими требованиями.

АҢДАТПА

Осы жобада «PC4U» ЖШС ақпараттық ортасына ЖБК «Инспектор» қорғау жүйесі енгізілді.

Бұл процесте құпия бағдарламалық жасақтаманың және аппараттық шешімдердің енгізілуін талап ететін, ұйымның ақпараттық ортасына қолжетімділіктің шектелуінен қорғаудың өзекті мәселесі талданды.

«Экономика» бөлімінде жүйенің құрылысы мен іске асырылуы үшін шығындар есептелді.

«Өмір қауіпсіздігі» бөлімінде тиісті сынақтармен жұмыс жағдайлары есептелді.

ANNOTATION

In this project, the protection system of the HSC “Inspector” was introduced into the information environment of «PC4U» LLP.

In the process, the actual problem of protecting against the leakage of confidential information and limited access to the information environment of organizations was analyzed, which requires the introduction of new software and hardware solutions.

In the “Economy” section, costs were calculated when constructing and implementation of the system.

In the section "Life Safety" was calculated the working conditions with the corresponding tests.

Содержание

Введение

Актуальность темы дипломной работы. Бурное развитие информационных технологий в сфере промышленных предприятий (ПП) привело к увеличению числа проблем, связанных с информационной безопасностью (ИБ). В настоящее время в связи с повышением уровня открытия информационной системы (ИС) и увеличением интенсивности обмена с пользователями и внешними ресурсами наблюдается снижение безопасности системы. Это обстоятельство может привести к большим финансовым потерям для организации. В связи с этим производственная компания, как и любая коммерческая организация, будет уместна для проведения исчерпывающего анализа защиты и рисков интеллектуальной собственности, что позволит оценить уровень потенциальных потерь, а также определить оптимальный способ защиты информаций.

Промышленные предприятия представляют собой инфраструктуру, которая содержит конфиденциальные данные и содержит информацию другого характера, которую необходимо защитить. Увеличение числа атак на информационную систему компании предъявляет свои собственные требования к защите информационных ресурсов и имеет задачу создания собственной интегрированной системы безопасности. Их решение определяет наличие нормативной базы, создание концепции безопасности, организационную работу и внедрение инструментов средств защиты информации (СЗИ) в компании. Эти основные компоненты определяют согласованную политику информационной безопасности.

Качественное создание безопасной информационной системы заключается в выборе оптимального метода защиты информации, соответствующего всем параметрам критерия эффективности и учитывающего наличие уязвимостей и взаимосвязей между ними. В связи с этим, одной из самых актуальных задач, которые стоят сегодня перед разработчиками и персоналом технического сопровождения информационной системы является полное решение проблемы ИБ ИС от создания концепции, политики ИБ организации до разработки определенных методов и рекомендаций по обеспечению ИБ.

Качественное создание защищенной информационной системы заключается в выборе оптимального метода защиты информации, отвечающего всем параметрам критерия эффективности, и учета наличия уязвимостей и взаимосвязей между ними. В этом смысле одной из наиболее неотложных задач для разработчиков и сотрудников службы технической поддержки информационной системы является полное решение проблемы информационной системы ИС, от концепции организаций и информационных политик до разработки определенных методов, и рекомендаций для обеспечения информационной безопасности.

Объектами защиты информационной системы являются сервера, защита интеллектуальной собственности, консоль управления учетными записями,

сервера и ЛВС, бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные.

Данная дипломная работа посвящена представлению системы руководящих принципов, правил, технологий и процедур информационной безопасности информационной системы, а также описанию высокоэффективных методов обеспечения информационной безопасности, основанных на внедрении технологии предотвращения утечки данных (DLP).

Научным новшеством диссертации является внедрение лучшего метода защиты информации в информационную систему с учетом уязвимостей и различных угроз, а также концепции и политики безопасности корпоративной информации.

1 Системный анализ уязвимости системы обеспечения информационной безопасности современного предприятия

1.1 Роль информатизации рабочего процесса

Информационная среда (ИС) – это организационно-техническая система, которая реализует информационные технологии и использует аппаратное и программное обеспечение, а также другие виды программного обеспечения для обнаружения и распространения информационных процессов для сбора, обработки, хранения, архивирования информации. Географически распределенные ИТ-системы составляют основу информационной системы программного обеспечения [1].

Особенность компании как объекта компьютеризации заключается в форме деятельности нескольких профилей, множестве форм и методов производственной работы, пространственном распределении в сложной инфраструктуре. Кроме того, следует отметить, что существует развитая структура дополнительных подразделений и услуг, необходимость адаптации к постоянно меняющемуся рынку производственных услуг, необходимость анализа рынка труда, электронного взаимодействия с другими организациями и частые изменения в уставе работников [2].

В области производственной или организационной деятельности информационная система ориентирована на новые результаты. Одним из важных результатов является уровень компетентности в области информации и коммуникации работников, который является одной из важнейших, важнейших характеристик качества специализированной подготовки, которая включает в себя деятельность, индивидуальные навыки человека. Эти способности определяют:

– возможности и умения самостоятельно искать, собирать, анализировать, представлять, передавать информацию;

– моделировать и проектировать объекты и процессы;

– ориентироваться в организационной среде на базе современных информационно-коммуникационных технологий (ИКТ);

– ответственно реализовывать свои планы, квалифицированно применяя современные средства ИКТ;

– использовать в своей практической профессиональной деятельности ИКТ.

В современной бизнес-системе информация непрерывно перемещается, способствуя разрешению продуктивной, административной и организационной деятельности. Наличие сложной информационной инфраструктуры с использованием новых информационных технологий обуславливает эффективную и качественную работу и управление компанией. Это чрезвычайно важно для создания баз данных информационных ресурсов, которые содержат нормативную информацию, производственную

информацию, справочные материалы и другую структурированную информацию [3].

Компьютеризация оказывает большое влияние на формы, методы, организацию и содержание всех областей и процессов производственной компании. Современное общество не может функционировать без современных средств и методов автоматической обработки информации с учетом его информационной инфраструктуры, и видов деятельности. Управление качеством продукции в компании осуществляется с помощью новых информационных технологий.

Качественное производства достигается в условиях грамотного обращения персонала с информационным пространством. Эффективным средством обеспечения этих условий является внедрение или разработка фирменных информационных систем и автоматизация рабочих процессов.

1.2 Общая структура построения информационной системы предприятия на базе ТОО «PC4U»

Информационная система инновационного предприятия входят следующие подсистемы:

– материально-техническое и программное обеспечение;
– информационно-технологическое обеспечение;
– информационно-ресурсное обеспечение;
– методическое обеспечение;
– организационное обеспечение;
– кадровое обеспечение;
– подсистема управления.

Подсистема материально-технического и программного обеспечения производственного процесса включает оснащение производственных помещений, помещений для офисной работы, необходимыми аппаратными устройствами и программным обеспечением, доступом к Интернету и локальной сети предприятия (рисунок 1) [4].

Рисунок 1 – Структура информационной среды предприятия

Подсистема информационно-технологического обеспечения представляет собой набор инфо-коммуникационных технологий, которые используются в производственном процессе и составляют основу соответствующих ресурсов (рисунок 1).

Подсистема информационно-ресурсного обеспечения является основой обеспечения содержания производства. Наполнение данной подсистемы ИС направлено на обеспечение офисов и сотрудников предприятия, исследовательской деятельности, выполнения производственных проектов на предприятии.

Подсистема методического обеспечения включает учебно-методические комплексы, пособия, учебные планы, интернет - материалы, предназначенные для разных участников производственного процесса.

Подсистема организационного обеспечения включает систему форм производственной деятельности в условиях ИС, обеспечивает организацию и доступ к остальным подсистемам ИС, дистанционную поддержку и коммуникацию участников производственного процесса.

Функционирование данной подсистемы ИС предполагает использование единой базы состава сотрудников предприятия, вспомогательного и административного персонала предприятия, содержащей профессиональные данные, сведения об производственных материалах [5].

Ниже приведена внутренняя структура организаций (рисунок 2).

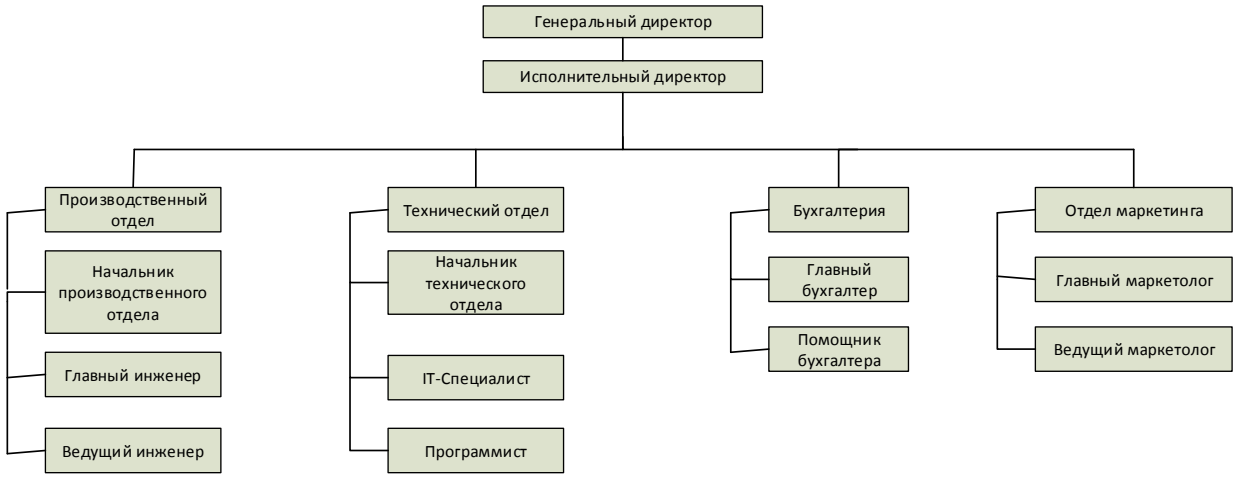

Рисунок 2 – Внутренняя структура управления ТОО PC4U

Интегрированная информационная среда ТОО «PC4U» основывается на системе учетных записей пользователей, для которых определены права и привилегии работы в среде, называемая служба каталогов Active Directory (AD) от Microsoft и база данных зарегистрированных пользователей к информационным ресурсам предприятия. Система единой регистрации пользователей информационных ресурсов предприятия позволяет системному

администратору регистрировать учетные записи в AD и в базе данных зарегистрированных пользователей веб-ресурсов предприятия [6].

Mikrotik RB951 представляет собой систему, включающую брандмауэр, VPN-сервер предназначенное для защиты корпоративных сетей предприятия.

Основные возможности этого маршрутизатора:

– собственно межсетевой экран 3 уровня;

– возможность быть точкой доступа

– встроенный VPN-сервер;

– поддержка всех технологий доступа в Интернет: DSL, ISDN, кабельных, спутниковых, беспроводных и диалап-соединений;

– поддержка VoIP и UPnP;

– возможность удаленного администрирования.

В информационной системе ТОО PC4U имеется 1 внутренняя локальная сеть.

Информационная система функционирует на базе 1 сервера, 1 маршрутизатор, 1 IP-телефония, GSM-шлюз и неуправляемых коммутаторов в различных кабинетах организаций.

В IT-инфраструктуре организаций имеется удаленный сервер через которую происходить работа с корпоративной почтой. Маршрутизатор со встроенной фаерволом 3 уровня нужна для того чтобы обеспечивать сотрудников доступом в интернет, а также возможно дать доступ во внутреннюю сеть предприятия из сети Интернет. IP-телефония позволяет сотрудником связываться друг с другом с помощью корпоративной связи. GSM-шлюз служит с целью объединения сотовой и проводной телефонной сети, помимо этого позволяет соединиться с мини-АТС.

К общий локальной сети подключены все кабинеты организаций. В организации присутствует 13 рабочих станций, из них 10 – ноутбуки и 3 – стационарные компьютеры.

1.3 Комплексное обеспечение информационной безопасности

1.3.1 Концептуальные положения политики информационной безопасности

Политика информационной безопасности (ПИБ) состоит из набора документов, требований и правил для защиты информации в корпоративной системе (КС) и используемых в ней информационных ресурсов.

Особенность информационной безопасности в информационной системе заключается в том, что компания представляет собой организацию с конфиденциальными данными и интеллектуальной собственностью, а также целью вторжения для несанкционированного доступа.

Основными причинами повышения информационной безопасности в корпоративной структуре являются:

Первая причина связана с различными группами пользователей, поскольку современная компания со своим собственным внутренним IP-

адресом является гетерогенной средой, в которой находятся интересы и данные различных групп пользователей.

Вторая причина связана с тем, что у компании могут быть информационные системы, к которым можно получить доступ через внешнюю сеть. ПК, смартфоны, планшеты и другие мобильные устройства оказывают значительное влияние на изменение рабочих процессов и предоставляют возможность доступа к информационным ресурсам компании из любой точки мира.

Третья причина – защита информационных систем и информации с ограниченным доступом.

Четвертая причина связана с актуальной проблемой: растущее число угроз.

Безопасность информационной системы предприятия можно рассматривать, исходя из трех направлений:

– в первую очередь, это информационная безопасность ПК, локальной сети, серверов и информационных систем. В современной организации используются несколько автоматизированных информационных систем (АИС) и около тысяч компьютеров, объединенных в локальную сеть, почтовые и файловые сервера. Безопасность ИС направлена на защиту от несанкционированного доступа, от вирусов, компьютерных атак и контроль разграничения прав доступа сотрудников;

– защита персональных данных сотрудников и конфиденциальной информации; [6]

– минимизация финансовых, репутационных, правовых рисков организаций.

Для обеспечения рабочего процесса на предприятии используются информационные ресурсы, включая документацию и информационные потоки. Это база данных клиентов, коммерческие предложения, контракты, список партнеров, рабочие программы, электронные журналы, заказы, заказы и другие важные ресурсы. Для правильного функционирования компании важно учитывать не только высококвалифицированный персонал, но и безопасность информационных ресурсов и системы. Все материалы являются официальными и требуют особого отношения. Некоторые материалы не публикуются, другие требуют специального использования. Это показывает, что компания обрабатывает информацию на разных уровнях доступа и с разными функциями. С точки зрения организации и использования распространения, эта информация делится на два основных типа (рисунок 3):

Общедоступная информация не составляет какую-либо тайну, определенную законодательством, либо уставом предприятиям и не требуют контроля безопасности. К ним можно отнести информационные блоки, статистическая информация и другие материалы.

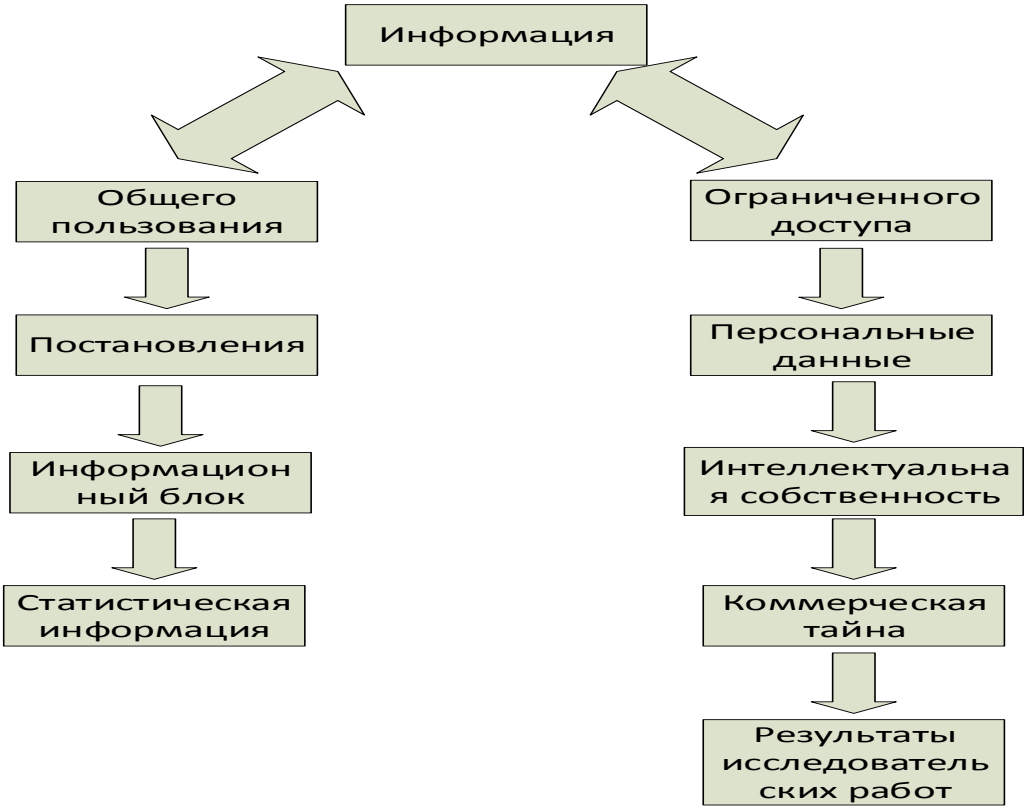

Рисунок 3 – Классификация информационных ресурсов по типу распространения и использования

К информации ограниченного доступа относится:

– персональные данные сотрудников(пользователей);

– данные, составляющие коммерческую тайну;

– разработанные предприятиям материалы, представляющие собой интеллектуальную собственность;

– приобретенные предприятиям программные обеспечения или лицензии, кража которых может ухудшить статус предприятия в конкурентной борьбе, либо повлечь за собой наступление уголовной или административной ответственности;

– научно-исследовательские и опытно-конструкторские работы, которые предприятия может проводить по заказу коммерческих или государственных заказчиков.

Современную модель обеспечения ИБ можно представить в форме многоуровневой документированной программы:

– верхний уровень включает утвержденные стратегии ИБ и составляющие ее различные отдельные политики ИБ;

– средний уровень включает обязательные базовые стандарты и рекомендуемые руководства;

– нижний уровень представлен отдельными технологиями и средствами защиты ИБ, а также многочисленными параметрами защищенности системы.

– новые технологии обеспечения защиты ИС дают возможность учебным заведениям решать задачи в следующих основных направлениях:

– организация защищенного доступа к материалам и системам из любой точки мира;

– защита информации ограниченного доступа и защита интеллектуальной собственности;

– выполнение требований законодательства в области ИБ ИС.

1.3.2 Требования к формированию политики безопасности

Информационная безопасность корпоративной системы обеспечивает противодействие любому несанкционированному вторжению в ее функционирование, а также попыткам изменения, хищения, выведения из строя или уничтожения ее компонентов, то есть защиту всех ресурсов данной системы.

Три группы проблем, являющиеся наиболее актуальными при анализе защиты информации и информационной системы [16]:

– нарушение конфиденциальности информации;

– нарушение целостности информации;

– нарушение доступности.

Для обеспечения безопасного функционирования информационной образовательной среды в архитектуре ее построения можно выделить три уровня:

– оборудование вычислительной сети, каналов и линий передачи данных, рабочих мест сотрудников, системы хранения данных;

– операционные системы, сетевые службы и службы по управлению доступом к информации, программное обеспечение;

– прикладное программное обеспечение, информационные сервисы и системы, направленные на пользователей (сотрудников).

Необходимым условием развития комплексной информационной сети (КИС) является согласование требований по защите интеллектуальной собственности для отдельных технологий. На втором уровне корпоративная система управления идентификацией многих компаний представляет собой отдельную и плохо связанную подсистему с разнородными операционными средами, которые согласуются только с точки зрения настройки IP-адресов или обмена данными. Отсутствие утвержденной архитектуры и непоследовательное развитие центра развития приводят к слабой системной организации КИС.

Особые требования предъявляются к работе пользователя или процесса в автоматизированной системе, и принимаются некоторые меры:

- идентификация и аутентификация;
- авторизация и доступ;
- конфиденциальность данных безопасности и прочих данных;
- целостность данных;
- доступность данных;

– аудит и мониторинг.

У каждого бизнеса должен быть четкий план развития ИТ, общие требования к ИС, политики информационной безопасности и утвержденные правила для ключевых компонентов ИТ. Обладая всеми необходимыми ресурсами, университет можно считать надежным административным ядром в управлении и высоким авторитетом ИТ-менеджера.

1.3.3 Классификация источников угроз информационной безопасности

Внутренняя инфраструктура организаций имеет свои особенности и проблемы комплексной информационной безопасности его корпоративных сетей гораздо шире, разнообразнее и острее, чем в других системах. Основные причины:

– при построении корпоративной сети многих организаций возникают проблемы со «скудным финансированием», выделяется мало средств на ее полную защиту;

– корпоративные сети рассматриваются с позиции настоящих на тот момент задач, так как не имеют стратегических целей развития;

– корпоративные сети организаций создавались для различных задач и в течение длительного промежутка времени. Поэтому они разнородны как по оборудованию, так и по программному обеспечению;

– в настоящее время планы комплексной информационной безопасности ИС, как правило, либо отсутствуют, либо не соответствуют современным требованиям.

При анализе безопасности ИС возможны как внутренние, так и внешние угрозы:

– попытки несанкционированного администрирования баз данных;

– исследование сетей, несанкционированный запуск программ по аудиту сетей;

– запуск игровых программ;

– установка вирусных программ и троянских коней;

– попытки взлома информационной системы «ВУЗа»;

– сканирование сетей, в том числе других организаций, через Интернет;

– попытки проникновения в системы бухгалтерского учета;

– поиск «дыр» в ОС, firewall, Proxy-серверах, на официальном сайте организаций;

– попытки несанкционированного удаленного администрирования ОС;

– сканирование портов и другие.

Основными элементами канала реализации угроз безопасности являются:

– источник угрозы;

– среда распространения сигнала, который носит защищаемую информацию;

– носитель защищаемой информации.

По виду возможных источников угрозы могут быть созданы:

– нарушителем (внутренним или внешним);

– аппаратной закладкой;

– опасными (вредоносными) программами;

– По виду нарушаемого свойства информации угрозы бывают:

– по конфиденциальности информации;

– по целостности информации;

– по доступности информации.

По типу информационных систем, на которые направлены угрозы бывают:

– угрозы, обрабатываемые в ИС на базе АРМ;

– угрозы, обрабатываемые в ИС на базе локальной сети;

– угрозы, обрабатываемые в ИС на базе распределенных информационных систем;

По способам реализации угрозы бывают:

– специальных воздействий на информационную систему;

– НСД в ИС;

– утечки информации по техническим каналам.

Источниками угроз информации могут выступать:

– рабочие станции неквалифицированных в сфере ИБ сотрудников;

– подключение сторонних людей к точке доступа организаций;

– интернет.

Согласно анализу, можно определить процент исходной статистики и источников угроз информационной безопасности. В 79% случаев это мужчины и только 17% женщины. Возраст от 36 до 45 лет составляет 37% мошенников, в следующей возрастной группе от 46 до 55 лет это 31% захватчиков. Можно видеть, что большой процент потенциальных мошенников составляют люди среднего возраста, причем самая молодая возрастная группа 18-25 лет составляет 1% преступников.

Около 65% случаев ИБ сообщают сотрудники внутренней организации, а 21% - бывшие сотрудники. Можно сделать вывод, что злоумышленники - это лица, которые знакомы с внутренней структурой компании, со всеми тонкостями рабочего процесса и знают о возможных слабостях и недостатках защиты.

Согласно проведенным расследованиям, причиной угрозы в большинстве случаев (62%) является отсутствие внутреннего контроля, а в 38% случаев злоумышленники имеют привилегии, чтобы обходить защитные меры. (рисунок 4).

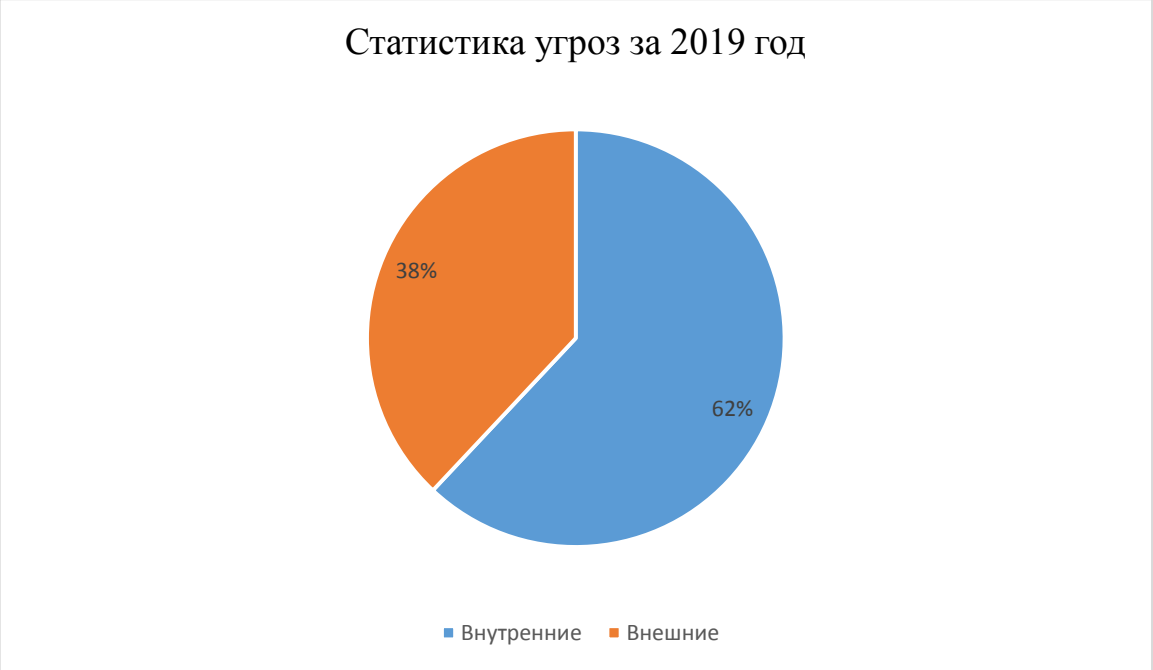

Рисунок 4 – Статистика угроз за 2019 год

Организациям могут угрожать различные риски.

Финансовые риски:

– риски, которые могут повлиять на финансовое состояние предприятия;

– безвозмездный убыток предприятия.

Правовые риски

Неконтролируемая публикация конфиденциального документа за пределами корпоративной сети может тщательно контролироваться регулирующими органами. Судебные иски и наказания за нарушения законов о защите персональных данных и других видов конфиденциальной информации не являются редкостью.

Репутационные риски

Риски, которые могут негативно повлиять на имидж организаций и подорвать отношение и уважение партнеров.

1.3.4 Общий анализ методов обеспечения защиты информационной системы предприятия.

Информационная безопасность системы производственного предприятия обеспечивается следующими формами защиты (рисунок 5):

– теоретические методы;

– правовые и организационные методы;

– сервисы сетевой безопасности;

– технические методы.

Рисунок 5 – Основные методы обеспечения информационной безопасности

Основой правовой формы обеспечения информационной безопасности производственного предприятия являются:

– закон «О персональных данных и их защите» от 21 мая 2013 года;

– закон Республики Казахстан от 11.01.2007 №217 – III «Об информатизации»;

– закон Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах» (с изменениями и дополнениями по состоянию на 02.04.04 г.);

– закон Республики Казахстан от 26 июня 1998 года № 233-I «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 14.10.2005 г.);

– концепция информационной безопасности Республики Казахстан». Одобрена Указом Президента Республики Казахстан от 10 октября 2006 года, № 199;

– указ Президента Республики Казахстан от 14 марта 2000 г. N 359 «О Государственной программе обеспечения информационной безопасности Республики Казахстан на 2000-2003 годы»;

– международный стандарт ISO/IEC FDIS 17799:2005. Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью;

– СТ РК 34.005-2002. Информационная технология. Основные термины и определения.

Классификация методов защиты информации (рисунок 6).

Препятствование – метод защиты ИС, с помощью которого у злоумышленника нет возможности попасть на защищаемый периметр.

Управление доступом – метод защиты, при котором регулируется и контролируется использование ресурсов ИС.

Маскировка – метод защиты, который предусматривает шифрование информации.

Регламентация – совокупность правил, норм, стандартов и процедур, применяемые при обработке информации, существенно затрудняющие действие атак и влияния других факторов.

Принуждение – создание условий, при которых сотрудники вынуждены соблюдать условия обработки информации под угрозой ответственности.

Побуждение – создание условий, при которых сотрудники не нарушают по их психологическим соображениям.

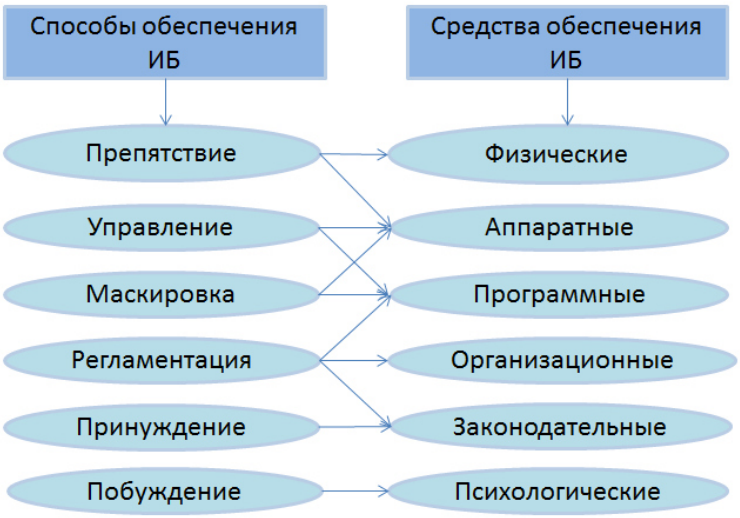

Рисунок 6 – Соответствие способов и средств защиты информации

Идентификация и аутентификация пользователей

Доступ к данным защищенной ИОС реализуется только после того, как пользователь проходит процесс представления этой системе, включающий три стадии:

– идентификация – сотрудник сообщает системе по ее запросу свое имя (идентификатор);

– аутентификация – пользователь подтверждает идентификацию, вводя никому не известную информацию (пароль);

– авторизация – предоставление возможности доступа к определенным информационным ресурсам.

Разграничение доступа

Когда информационная система встроена в организацию, роли распределяются и доступ сотрудников к информационным ресурсам ограничен. Сначала администратор решает, могут ли пользователи получать доступ к определенной информации в сети. Несколько сложнее организовать

доступ к базе данных, где она может быть распределена по отдельным частям в соответствии с правилами. Получив доступ сотрудника к определенным ресурсам, администратор устанавливает операции, которые может выполнять пользователь.

Можно выделить следующие операции с файлами:

– чтение (R);

– запись;

– выполнение программ (E).

Протоколирование и аудит

Запись и тестирование являются одной из важных функций, которые должны присутствовать во всех системах безопасности. Реестр собирает и собирает информацию обо всех инцидентах, которые происходят в информационной системе. В обзоре анализируется вся собранная информация. Целью этого процесса является мониторинг соответствия системы или сети требуемым правилам и стандартам безопасности. Аудит обеспечивает анализ всех аспектов защиты информации и информационных систем, а также угроз, которые могут привести к проблемам безопасности.

Антивирусная система

Работа антивирусных программ осуществляется по следующему принципу:

– предотвращение;

– обнаружение;

– удаление.

Когда на ПК появляются новые файлы или приложения или в Интернете меняются настройки просмотра, вы используете электронную почту и другие интернет-ресурсы.

VPN

Виртуальные частные сети – это полные протоколы и технологии, которые помогают вам организовать частную виртуальную сеть на вершине глобальной сети. Они состоят из арендованных каналов связи от различных телекоммуникационных компаний и интернет-провайдеров. Эти каналы связи соединяют только два объекта, отделенных от остальной части трафика, поскольку арендованные каналы обеспечивают двунаправленную связь между двумя сайтами. [8].

Виртуальные частные сети обладают следующими особенностями:

– трафик шифруется, чтобы обеспечить защиту от НСД и прослушивания;

– выполняется аутентификация удаленного сайта;

– при развертывании виртуальных частных сетей используется множества протоколов.

Firewall

Брандмауэр – это устройство контроля доступа к сети, которое блокирует весь трафик, кроме разрешенных данных. Брандмауэры позволяют вам разделить сеть на две или более частей и обеспечивают защиту от несанкционированного доступа к сетевой информации, транспортных уровней и использования семи сетевых протоколов модели OSI. Уровень. Трафик, проходящий через межсетевой экран, может быть настроен службами, IP-адресами отправителя и получателя и идентификаторами пользователей, запрашивающими службу.

IDS и IPS

Система обнаружения вторжений (СОВ) – это программный или аппаратный инструмент, который обнаруживает несанкционированные попытки проникновения в защищенную зону. Защищенный периметр - это виртуальный периметр, в котором размещены компьютерные системы. Эта область может быть определена межсетевыми экранами, точками разделения или рабочими столами с модемами.

Системы предотвращения вторжений (IPS) аналогичны IDS. Основное отличие заключается в том, что IPS работает в режиме реального времени и автоматически блокирует атаки в сети. Каждая система IPS содержит модуль IDS.

Использование IPS-систем реализует следующие задачи:

– обнаружение сетевых атак и их предотвращение;
– прогноз возможных будущих атак и анализ имеющихся уязвимостей;
– выполнение отчета по существующим угрозам;
– получение полезной информации об инцидентах ИБ;
– определение расположения внутренних и внешних источников атак.

DMZ зона

Суть демилитаризованной зоны (DMZ) заключается в том, что она не входит во внутреннюю или внешнюю сеть и доступна только в соответствии с предварительно определенными правилами брандмауэра. Только серверы находятся в зоне DMZ.

Основная цель зоны DMZ – предотвратить доступ внешней сети к ресурсам и компьютерам внутренней сети, поскольку локальная сеть удаляется в определенной области всех служб, требующих доступа из внешней среды.

Криптографические методы защиты информации

Криптографическая защита информации – это трансформация исходной информации, которая недоступна сотрудникам без прав доступа.

Существует несколько подходов к классификации методов преобразования криптографической информации. Методы

криптографического преобразования информации, влияющие на информацию об источнике, делятся на четыре типа (рисунок 7).

Рисунок 7 – Классификация методов криптографического преобразования информации

Вывод по первой главе:

Информационная среда компании является областью сетевого взаимодействия для всех участников рабочего процесса, где одним из ключевых вопросов является обеспечение безопасности ИС.

В этой главе было рассмотрено проектирования информационной среды ТОО «PC4U», проанализируем уязвимость системы информационной безопасности современного предприятия, а также рассмотрим существующие средства и методы защиты информации о ее ключевых преимуществах и недостатках.

Выявленные противоречия и недостатки различных методов защиты информации позволили сформулировать задачу исследования: выявить пути повышения безопасности информационной среды организации.

Основные задачи, которые решаются во второй главе:

– анализ и обоснование системы мониторинга и контроля действий в информационную среду ТОО «PC4U», учитывая особенности обоих систем.

2 Анализ и обоснование оптимального технического метода защиты

2.1 Выбор и обоснование внедрения оптимального метода защиты в информационную систему

В соответствии с Законом Республики Казахстан «Об информатизации», Законом Республики Казахстан «О персональных данных и их защите» должны использоваться меры по защите персональных данных от раскрытия, меры по защите электронных информационных ресурсов и систем контроля доступа, а также для записи данных о доступе к информации.

Защита персональных данных включает в себя ряд технических, организационных, теоретических и правовых мер по защите персональных данных (сотрудников).

В соответствии с Законом Республики Казахстан «О персональных данных и их защите» сбор, обработка и защита персональных данных осуществляются в соответствии с принципами:

1) соблюдения конституционных прав и свобод человека и гражданина;
2) законности;
3) конфиденциальности персональных данных ограниченного доступа;
4) равенства прав субъектов, собственников и операторов;
5) обеспечения безопасности личности, общества и государства.

В силу Постановления Правительства от 20 декабря 2016 года № 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», организациям необходимо производить мониторинг действий пользователей и персонала, производить мониторинг использования средств обработки информации и регистрацию событий и инцидентов, а так же осуществлять другие действия по контролю и защите информации.

По Постановлению Правительства от 20 декабря 2016 года № 832 регистрация инцидентов информационной безопасности требует:

– автоматическое создание журналов действий администраторов;
– применения системы мониторинга инцидентов и событий ИБ;
– оповещения на основе автоматического определения подозрительного события или инцидента ИБ.

На этапе опытной и промышленной эксплуатации объектов информатизации должны использоваться средства и системы:

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

По условиям стандарта СТ РК 1699-2007 – системы контроля и управления доступом должны соответствовать всем необходимым требованиям и дополнительно обеспечивать [9]:

– регистрацию и протоколирование подозрительных и текущих сообщений;

– отображение подозрительных событий;

– защиту технических и программных средств от несанкционированного доступа;

– автоматический контроль исправности средств, входящих в систему, и линий передачи информации;

– возможность автономной работы контроллеров системы;

– блокировку прохода по точкам доступа командой с пункта управления в случае нападения;

– возможность подключения дополнительных средств специального контроля, средств досмотра.

Основными техническими методами защиты является в информационной системе ТОО «PC4U»:

1) управление доступом;

2) регистрация и мониторинг действий ПК;

3) обеспечение целостности;

4) антивирусная защита;

5) защита и контроль информационной компьютерной сети.

Согласно проведенному анализу информационной безопасности организации ТОО «PC4U», изучения информационных ресурсов, было выявлено, что управление доступом обеспечивается службой каталогов Active Directory, антивирусная защита обеспечивается антивирусным программным обеспечением Антивирус Касперского, базовая защита информационной компьютерной сети обеспечивается системой Mikrotik.

Технология Active Directory – это служба каталогов, созданная Microsoft. Служба каталогов хранит информацию обо всех сетевых ресурсах, содержит данные в упорядоченном формате и предоставляет им надлежащий доступ. Клиенты могут отправлять конкретные запросы Active Directory для получения информации обо всех объектах в сети.

В список возможностей Active Directory входят следующие основные функции:

– безопасное хранение данных. В каждом объекте в Active Directory имеется личный список управления доступом (ACL – Access Control List);

– многофункциональный механизм запросов, основанный на глобальном каталоге (GC), созданный AD. Все сотрудники, работающие в AD, могут обращаться к этому каталогу;

– синхронизация данных упрощает доступ к информационным ресурсам, повышает степень ее доступности и надежность всей службы;

– концепция комплексного расширения, дающая возможность добавлять новые типы объектов, дополняя существующие объекты;

– сетевое взаимодействие с применением нескольких протоколов. Служба Active Directory основана на модели X.500, благодаря чему поддерживаются такие сетевые протоколы, как LDAP 2, LDAP 3 и HTTP;

– для реализации службы имен контроллеров доменов и поиска сетевых адресов используется служба DNS (Domain Name System – система доменных имен).

Антивирус Касперского является продуктом, предназначенный для защиты персональных компьютеров от вирусов вредоносных программ, троянских программ, шпионских программ, а также неизвестных угроз с помощью защиты в режиме реального времени, включающей компонент HIPS. Суммарный комплекс программы включает: файловый, почтовый и веб антивирусы.

Антивирус Касперского – это продукт, предназначенный для защиты персональных компьютеров от вирусов, троянов, шпионских программ и неизвестных угроз, использующих защиту в режиме реального времени, включая компонент HIPS. Общая программа включает в себя: файлы, электронную почту и веб-антивирус.

Антивирус Касперского включает:

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

– задачи проверки на вирусы, которые проверяют компьютеры или отдельные файлы, каталоги, тома и документы на наличие вирусов;

– сервисные функции, обеспечивающие информационную поддержку при использовании программы и позволяющие расширить ее функциональные возможности;

– обеспечивает защиту пользователя от вирусов.

Особенности Антивируса Касперского:

– безопасность рабочих станций, которые выполняют многоуровневую защиту, обновления системы безопасности, защиту от угроз, предотвращение и блокирование сетевых атак, облачную интеграцию;

– безопасность файловых серверов;

– предоставление централизованного управления.

Компьютерный вирус – это вредоносная программа, которая может дублировать процесс создания своих копий и вставки в код других программ, системной памяти, загрузочных файлов и секторов. Вирусы, которые запрограммированы для завершения программ, блокирования пользователей, уничтожения файлов и документов, а также для остановки систем ПК.

Основные источники вирусов:

– дискета, содержащаяся файлы и документы;

– компьютерная сеть, в том числе система электронной почты и Internet;

– зараженный вирусом жесткий диск;

– оставшийся в оперативной памяти вирус.

Miktorik является программным комплексом для обеспечения доступа локальной сети организации в Интернет. Для данного продукта характерны гибкая и быстрая настройка, интеграция в существующую сеть организации с поддержкой Active Directory и прочих программ Microsoft, высокий уровень защиты системы, поддержка построения корпоративной виртуальной сети через Интернет, простота администрирования и требований к ресурсам.

Программа Miktorik Firewall является межсетевым экраном 3 уровня, так как поддерживает правило только для ip-адресов. Такой фаервол не дает возможность анализа всего проходящего интернет-трафика, соответственно не сможет привести его в соответствий с политиками ИБ.

С помощью данного продукта установка виртуальной частной сети практически не сложно. Сервер и клиенты VPN являются составляющей частью возможностей Miktotik по безопасному удаленному доступу к корпоративной сети. Использование виртуальной сети Miktorik VPN дает возможность пользователям удаленно подключаться к любым ресурсам локальной сети [10]. Хотелось бы отметить, что встроенный NAT-технология в маршрутизаторы Mikrotik позволяет осуществить удаленное подключение к отдельно взятым объектом внутренний сети.

Метод защиты информационной системы, применяемый в организации ТОО «PC4U» не достаточно осуществляют контроль за персональным компьютером, невозможно расследовать инциденты с важными персональными и коммерческими данными, конфиденциальными информационными ресурсами.

Основными недостатками ИБ ИС ТОО «PC4U» являются отсутствие полного контроля следующих действии сотрудника:

– редактирования информации (в общей папке);
– отправка по электронной почте;
– отправка на печать;
– копирование информации;
– посещение web сайтов.

После анализа было решено, что для повышения информационной безопасности в техническом отношении и обеспечения требований законодательства Республики Казахстан, должна быть внедрена система мониторинга и контроля информации на персональных компьютерах.

Система мониторинга является одним из ключевых компонентов информационной безопасности, поскольку для любой организации важно знать информацию о выполненных операциях и какие действия эти действия предпринять. Эти системы представляют собой программное или аппаратное обеспечение, которое отслеживает действия пользователя, предотвращает утечку конфиденциальной информации, а также помогает определить нецелевое использование рабочего времени. Отслеживая все действия сотрудников за ПК, можно повысить качество работы сотрудников и повысить их эффективность.

Высокие стандарты качества и нормативные требования в большинстве крупных организаций в Казахстане требуют интегрированной системы мониторинга, обеспечивающей надежное хранение данных. Необходимость создания таких систем обусловлена увеличением внутренних (внутренних) угроз.

Система контроля и управления информацией на персональных компьютерах включает технологию предотвращения утечки данных (DLP).

Системы DLP – это аппаратные и программные технологии, которые могут предотвратить потерю конфиденциальной информации, случайно или намеренно созданной. Эти технологии работают в комплексе с другими несопоставимыми системами, используемыми для защиты информационной системы.

Набор функций, которые помогают идентифицировать и блокировать передачу информации из корпоративной системы в сеть:

– обеспечение фильтрации интернет-трафика, информационных потоков;

– обеспечение анализа контента по предварительно установленным ключевым словам, «оцифрованным» документам, определенным выражениям.

Применение DLP-систем дает возможность получить трехуровневую защиту от утечки конфиденциальной информации:

Data-in-Motion – защита информации в момент передачи данных по информационным каналам. При таком процессе осуществляется:

– оценка действующих протоколов передачи данных;

– контроль интернет – программ;

– фильтрация личной и рабочей почты;

– оценка интернет-трафика беспроводных систем;

– оценка безопасности FTP – соединения.

Data-in-Use – защита информации на коммуникационном оборудовании, используемом сотрудником.

Data-at-Rest – защита информации при ее хранении в памяти применяемого для работы IT-оборудования либо на серверах, а также в сетях хранения данных (СХД).

DLP-система при определении степени конфиденциальности информации образовательной системы основывается на различных методах:

– лингвистический анализ отправляемых данных;

– анализ статистики интернет-трафика;

– выявление шаблонных выражений;

– применение цифровых «отпечатков» секретных документов.

2.2 Техническая спецификация системы «Инспектор»

Система централизованного контроля действий, производимых на компьютерах (далее – СКДК) состоящая из контроля и мониторинга

запущенных программ, сбора сведений об установленном оборудовании и системы отчетности.

Согласно проведенному анализу в организации ТОО «PC4U» количество ПК – 13 шт. Система должна обеспечивать контроль не менее 200 пользователей и иметь следующий функционал:

Общие требования по управлению и отчетности СКДК:

1. Единая в рамках системы консоль отчетности, реализованная посредством веб-приложения.

2. Ролевая система администрирования, с возможностью делегирования полномочий по управлению и отчетности, с учетом организационной структуры.

3. Панель оперативного мониторинга в консоли управления, отображающая в реальном времени запущенных процессов на ПК.

4. Генерация SMTP оповещений для сигнализации действий при срабатывании определенных настраиваемых событий.

5. Архитектура системы должна предусматривать серверную аппаратно-программную часть (серверный модуль) и программную часть (клиентские модули) – Агенты для ПК.

Система должна иметь следующие возможности:

– мониторинг активного времени компьютера сотрудника;

– мониторинг программ;

– сбор отчетности по посещаемым сайтам;

– мониторинг вводимого текста;

– мониторинг файловых операций;

– регистрация изображения экрана (снимок экрана рабочего стола в определенный период времени или действии);

– мониторинг распечатываемых документов;

– мониторинг подозрительных действий и контроль оборудования;

– формирование отчетности.

Административная консоль – должна быть реализована в двух исполнениях: в виде веб-приложения для формирования отчетности и в виде консоли управления (отдельное ПО для управления, устанавливаемое на рабочее место ответственного сотрудника) для управления настройками системы.

Требования к модулю контроля использования данных СКДК:

Серверный модуль – должен позволять оперативно просматривать информацию об активности на компьютерах в режиме реального времени через веб-интерфейс, и формировать отчетность следующего характера:

– 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 текста и графики буфера обмена;

– статистика совершения подозрительных действий пользователями (запуск нежелательного ПО, посещение сайтов и пр.);

– активная реакция на подозрительные действия (выдача сообщения о несанкционированном действии и занесение результата в базу данных);

– генерация как сводных отчетов, так и по различным критериям;

– возможность экспорта отчетов в Excel;

– возможность удаленного администрирования (установки клиентской части ПО удаленно);

– хранение информации в собственной БД;

– возможность формирования группы отчетов;

– мониторинг рабочего стола в режиме реального времени.

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

Агенты для ПК (клиентский модуль) – должны устанавливаться на клиентских компьютерах и соответствовать следующим требованиям:

– иметь внутренние хранилище со сроком хранения до 36 часов в автономном режиме (без подключения к локальной вычислительной сети, через которую доступен серверный модуль);

– производить сбор информацию о производимых действиях на персональном компьютере, на котором установлен клиентский модуль и передавать на серверный модуль посредством локальной вычислительной сети по настроенному порту.

Агенты для ПК должны обеспечить полную совместимость с операционными системами: - Microsoft Windows® 10/ 8 / 7 /Vista/XP/2000 NT 4.0 (SP6), Server 2000, Server 2003 (32-bit & 64-bit), Server 2008 (32-bit & 64-bit) 2008 R2, Server 2012.

Агенты для ПК должны обеспечить инсталляцию и функционирование на рабочих станциях с оперативной памятью от 128 Мб для ОС Windows 2000, Windows XP, Windows 10.

Административная консоль должна предусматривать серверные и клиентские настройки, причем клиентские настройки должны делится на следующие группы:

– для компьютеров – настройки, которые воспринимаются компьютерами, но не пользователями, так как на одном компьютере могут работать несколько пользователей;

– для пользователей – настройки, которые воспринимаются отдельными пользователями компьютеров, но не самими компьютерами.

Производителями системы мониторинга и контроля действий на ПК, отвечающие данным требованиям, являются: InfoWatch, SearchInform, NeoSpy и Инспектор.

Таблица 2 – Сравнительная таблица производителей системы мониторинга и контроля действий на ПК

Название системы	InfoWatch	SearchInform	NeoSpy	Инспектор
1	2	3	4	5
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
Анализ по словарю	Да	Да	Нет	Да

Лингвистический анализ	Да	Да	Нет	Да

1	2	3	4	5
Блокируемые протоколы	HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S, IMAP4, IMAP4S	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, IMAP4S
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
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

1	2	3	4	5
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 метода защиты ИС ТОО «PC4U» был выбран отечественный продукт АПК «Инспектор», обладающий определенными преимуществами и не уступающим другим аналогичным продуктам.

– первым критерием является то, что АПК Инспектор не требует приобретения оборудования для обработки и хранения данных и дополнительного программного обеспечения (операционная система, база данных), в отличие от всех остальных производителей;

– в АПК Инспектор имеется поддержка морфологии казахского языка, что играет немаловажную роль при внедрении данной системы в любую организацию Казахстана;

– так как АПК Инспектор является отечественным продуктом, компания-производитель в рамках дипломной работы предоставляет продукт в учебных целях на льготной основе. Осуществление поддержки местными разработчиками существенно влияет на ход внедрения продукта. С экономической точки зрения внедрение АПК Инспектор выгодно, рассмотрение других продуктов возможно только с учетом демонстрационных версий с ограниченным периодом из-за их дорогой стоимости.

2.3 Аппаратно-программный комплекс системы «Инспектор»

Аппаратно-программный комплекс Инспектор – это комплексное решение для защиты важной бизнес-информации, система мониторинга и контроля действий, выполняемых пользователем на компьютере. Инспектор идеально подходит для крупного и среднего бизнеса, а для малого бизнеса можно использовать облачный сервис Инспектор [11].

Аппаратно-программный комплекс «Инспектор» – система информационной защиты, контроля, мониторинга и анализа действий, производимых на персональных компьютерах**.**

Программное обеспечение «Инспектор» – комплексное программное обеспечение: система защиты информации, контроля, мониторинга и анализа действий, выполняемых на ПК.

Система отслеживает запущенные программы и предоставляет информацию об установленных устройствах.

Предназначен для анализа эффективности использования рабочего времени пользователями персональных компьютеров и ИТ ресурсов в наглядных отчетах и может быть использован для предотвращения утечек информации через компьютерные сети, носители информации, устройства ввода-вывода, а также для анализа действий пользователей электронных устройств.

Предназначен для анализа эффективности рабочего времени пользователей ПК и ИТ-ресурсов в визуальных отчетах и предотвращения утечки информации через компьютерные сети, носители информации, устройства ввода-вывода, а также для анализа действий пользователей электронных устройств.

Аппаратно-программный комплекс необходим для использования в любой организации, где сотрудники работают за компьютерами.

Аппаратно-программный комплекс необходимо для руководителей, сотрудников отдела кадров, служб информационной безопасности и служб информационных технологий.

– основные функциональные возможности системы:
– мониторинг активного времени компьютера;
– мониторинг программ;
– сбор отчетности по посещаемым сайтам;
– мониторинг вводимого текста;
– мониторинг файловых операций;
– мониторинг снимков с экрана;
– мониторинг распечатываемых документов;
– мониторинг подозрительных действий и контроль оборудования;
– формирование отчетности (сводный отчет, мастер отчетов);
– возможность формирования группы отчетов;
– хранение информации в собственной БД;

– возможность удаленного администрирования (установки клиентской части ПО удаленно);

– мониторинг рабочего стола в режиме реального времени;

– активная реакция на подозрительные действия (выдача сообщения о несанкционированном действии и занесение результата в базу данных);

– система позволяет формировать отчетность следующего характера:

– время прихода/ухода пользователя (сотрудника), диаграмма активности в течении дня;

– список посещаемых сайтов (отображение активной / пассивной работы с ними);

– использование программ;

– контроль распечатываемых документов, электронной почты и почтовых вложений;

– мониторинг вводимого текста в программах, на сайтах, чатов;

– мониторинг операций с файлами, теневое копирование отправляемых через интернет и выводимых на флэш накопитель файлов;

– мониторинг поисковых запросов, текста и буфера обмена.

Аппаратно-Программный комплекс Инспектор (серверная часть). Предназначен для руководителя; позволяет оперативно просматривать информацию об активности на компьютерах в режиме реального времени, создавать задачи по формированию различных видов отчетов. Серверная часть имеет административную консоль, которая реализована в двух исполнениях: в виде веб-приложения для формирования отчетности и в виде консоли управления (отдельное ПО для управления, устанавливаемое на рабочее место ответственного сотрудника) для управления настройками системы (рисунок 8).

Рисунок 8 – Аппаратная часть системы мониторинга и контроля «Инспектор»

Административная консоль имеет серверные и клиентские настройки, причем клиентские настройки делятся группы например как:

– для компьютеров – настройки, которые воспринимаются компьютерами, но не пользователями, так как на одном компьютере могут работать несколько пользователей;

– для пользователей – настройки, которые воспринимаются отдельными пользователями компьютеров, но не самими компьютерами.

Программа агент (клиентский модуль). Устанавливается на компьютерах, за операциями которых необходимо вести наблюдение; собирает информацию о производимых действиях на персональном компьютере посредством функционала операционной системы и фиксации времени работы пользователя за персональным компьютером. Клиентский модуль позволяет производить сбор информации о производимых действиях на персональном компьютере, на котором установлен клиентский модуль, и передавать на серверный модуль посредством локальной вычислительной сети по настроенному порту. Имеет внутренние хранилище позволяющее хранить данные в автономном режиме. Программа агент обеспечивает полную совместимость с операционными системами: Microsoft Windows® 10 / 8 / 7 / Vista / XP / 2000 NT 4.0 (SP6), Server 2000, Server 2003 (32-bit & 64-bit), Server 2008 (32-bit & 64-bit) 2008 R2, Server 2012. Минимальные системные требования к персональному компьютеру для установки программы агента клиентского модуля: Процессор: 32/64 разрядный с тактовой частотой не ниже 1 Ггц, Оперативная память: 256 МБ, Графический процессор: SVGA (800x600), Операционная система: Windows XP, Windows 7, Windows 8-8.1 и выше.

В результате изучения характеристик АПК и технической спецификации требуемого решения можно принять решение о соответствии всем требованием. Кроме того были выделены основные преимущества внедрения АПК «Инспектор»:

– клиентский модуль не требователен к ресурсам. Клиенты системы не влияют на производительность ПК, так как вся обработка данных ведется на сервере, потому не возникает никаких сложностей при работе и использовании комплекса на любых компьютерах;

– локальное хранилище. При отсутствии связи с сервером данные наблюдений не пропадут, а будут накапливаться в локальной базе данных и гарантированно будут переданы на сервер после возобновления связи;

– отложенное наблюдение. При ограниченных каналах связи возможна настройка системы для передачи данных на сервер в определенное время или по запросу;

– удаленная и незаметная установка. Можно установить клиента на удаленные машины в скрытом от сотрудника режиме. При этом предусмотрены различные способы, в том числе через Active Directory;

– разграничение прав доступа. Возможность назначать права ответственным как на определенные отчеты, так и на выбранные отделы в иерархии компании;

– интеграция с Active Directory. Возможность автоматической синхронизации данных и структуры сразу с несколькими доменами компании, включая информацию о сотруднике;

– отправка отчетов. Возможность автоматической генерации отчетов по расписанию и сформированных отправки (по e-mail, FTP и др. способами).

– функции DLP для документов. Открытие, отправка в интернет, копирование на флэшку, в буфер обмена документов с ключевыми словами или фразами сопровождается событием (или запретом);

– возможность запрета флэш-дисков. Возможность запретить запись или полностью доступ к съемным носителям;

– реакция на подозрительные события. Выдача уведомлений о важных событиях пользователей в трее и окне браузера со звуком. Возможность получения SMS и e-mail уведомлений.

При детальном изучении АПК «Инспектор» был выделен следующий функционал для контролирующего сотрудника и технические особенности.

Административная консоль для формирования отчётности имеет три модуля (рисунок 9):

– «Онлайн» модуль для просмотра действий производимых на ПК в режиме онлайн (процессы, окна, экран рабочего стола в реальном времени) (рисунок 10);

– «Оффлайн» модуль для формирования отчётности на основе данных, которые находятся во внутренней базе данных комплекса и информации о действиях производимых на ПК ранее собранных с них с помощью клиентского модуля (рисунок 11);

– «Настройка» модуль нужен для того чтобы управлять и настраивать АПК «Инспектор (рисунок 12).

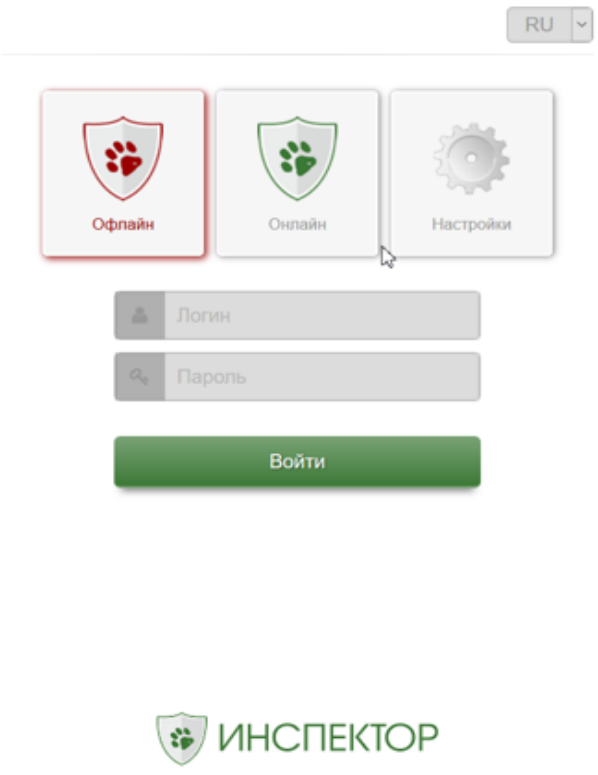

Рисунок 9 – Модули работы системы «Инспектор»

В модуле «Оффлайн» существует возможность формирования следующих отчетов:

1) Анализатор рисков. Анализатор, который настраивается на основе профилей и словарей показывает эффективную, неэффективную или вредную работу сотрудника;

2) Сводный отчет, наглядно представляющий общую статистику в области используемых ресурсов по сотрудникам;

3) Машинное время, определяющее время включенного состояния компьютеров сотрудников;

4) Пользовательское время, показывающее активность сотрудников за день, прогулы, опоздания на работу, популярные программы и сайты;

5) Программы, в которых активно работал сотрудник, а также время просмотра данных программ;

6) Сайты, которые посещал сотрудник;

7) Буфер обмена, содержащий передаваемые текст, файлы и картинки.

8) Интернет-запросы**.** Возможность просмотреть все поисковые запросы в различных «поисковиках» – Google, Yandex и другие;

9) Снимки экранов**.** Съем скриншотов с множеством настроек;

10) Видео снимков**.** Генерация непрерывного видео по скриншотам для просмотра через браузер или медиа-плеер;

11) Печать на принтере**.** Возможность перехвата распечатанных файлов в формате спулера и расчет стоимости в зависимости от установленного тарифа;

12) Файловые операции**.** Перехват копирования, удаления, переноса файлов. При копировании файлов на флэшку возможно теневое копирование;

13) Отправка файлов**.** Файлы, отправляемые через браузер, почтовые клиенты, Skype, Lync и популярные мессенджеры. Во всех случаях осуществляется перехват и сохранение файлов (с возможностью запрета отправки);

14) Письма (e-mail). Перехват входящих и исходящих электронных почтовых писем;

15) Чаты и звонки**.** Перехват сообщений и запись голосовых переговоров в Skype, Lync и Viber, а также сообщений Jabber;

16) Контакты**.** Возможность посмотреть список контактов сотрудника, с которыми он общался по переписке e-mail, Skype и в чатах;

17) Граф связей**.** Визуальное отображение отчета «Контакты» в виде удобного для просмотра графа;

18) События по пользователю и компьютеру**.** Запись в отчет тех событий, которые может сотрудник настроить (запуск программ, сайтов, ввод текста с учетом алгоритма неточного сравнения слов);

19) Оборудование/софт**.** Показывает изменения в составе оборудования на машинах и установленный/удаленный софт;

20) Установки программ**.** Возможность просмотра количества установок различного программного обеспечения по всей компании для выявления нелицензионного ПО;

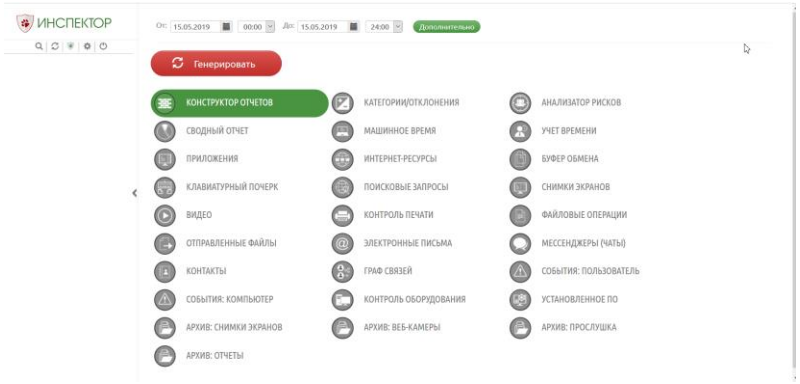

Рисунок 10 – Режимы работы системы «Инспектор» в модуле «Оффлайн»

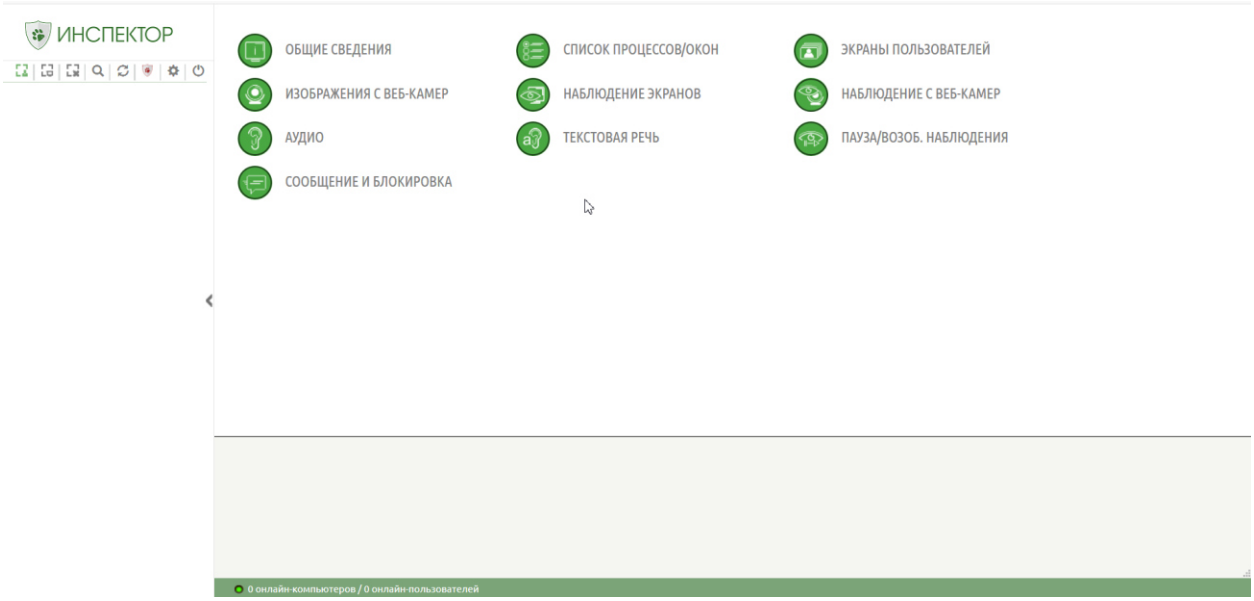

Рисунок 11 – Режимы работы системы «Инспектор» в модуле «Онлайн»

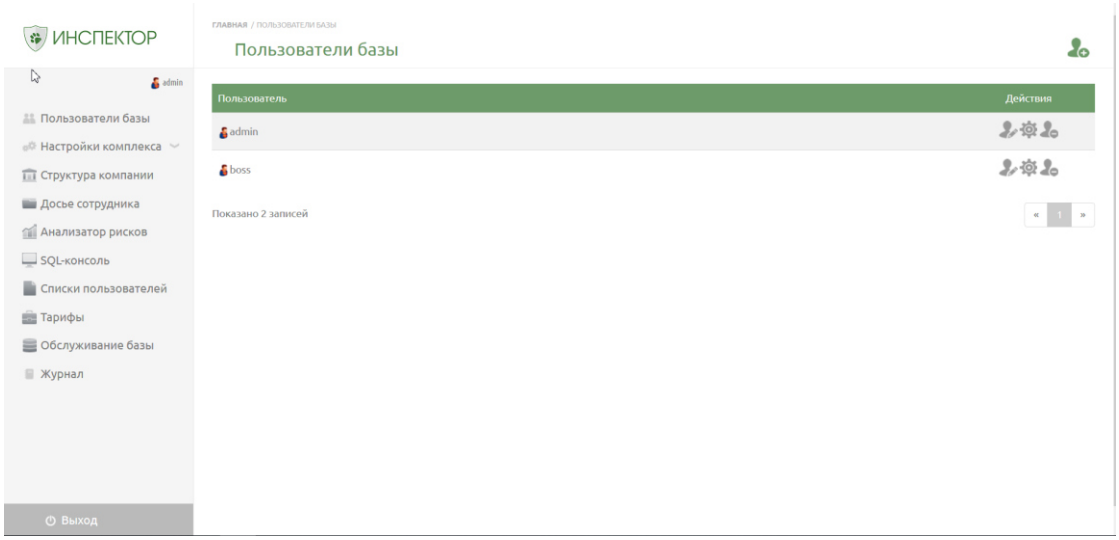

Рисунок 12 – Режимы работы системы «Инспектор» в модуле «Настройки»

Вывод по второй главе:

Во второй главе диссертации проведен анализ технических и дополнительных особенностей компаний-производителей продукта системы мониторинга и контроля действий пользователей на ПК: InfoWatch, SearchInform, NeoSpy и Инспектор. Согласно проведенному анализу, в качестве оптимального метода защиты информации был выбран отечественный продукт «Инспектор». Составлены технические требования к внедрению продукта «Инспектор» в информационной среде ТОО «PC4U». Данный продукт совместим в применении с системами защиты внутренней информационной системы предприятия: Active Directory, Антивирус Касперского и Miktorik.

Аппаратно-программный комплекс Инспектор является комплексным решением для защиты важной конфиденциальной информации, системой контроля и мониторинга действий, совершенных на компьютере пользователем.

Выше приведены сведения о важных параметрах и особенностях продукта «Инспектор» и его преимущества.

В общем, данная глава дипломной работы посвящена обоснованию выбранного оптимального метода, его анализу, изучению и составлению технических требований для внедрения системы мониторинга и контроля действий на ПК «Инспектор» в ИС ТОО «PC4U».

3 Технико-экономическое обоснование

Проект был посвящен организаций информационной безопасности предприятия и сделан с поставленными задачами. Объем знаний в сфере информационной безопасности позволял осуществить запланированный проект.

Технико-экономическое обоснование содержит следующие пункты:

– определение трудоемкости построения системы защиты;

– расчет затрат на внедрение системы защиты;

– определение ценности проекта;

– оценка результатов работы системы защиты.

3.1 Определение трудоемкости построения системы защиты

Для построения системы защиты проект был разделен на этапы, который также покажет трудоемкость реализуемого проекта. Форма разделения реализуемого проекта по этапам для определения трудоемкости приведена в таблице 3.1.

Таблица 3.1 – Этапы построения системы защиты

Этапы построения системы защиты	Вид работы	Трудоемкость, чел. час.
Этап 1	Постановка задач	15
Этап 2	Проектирование и утверждение ТЗ на проектирование системы защиты	30
Этап 3	Поиск и изучение подобных мер защиты	40
Этап 4	Поиск и изучение сопутствующей литературы	30
Этап 5	Реализация проекта	50
Этап 6	Отладка и устранение недоработок	35
Этап 7	Тестирование системы защиты	35
Этап 8	Подведение итогов по проектированию системы защиты	25
Итого: трудоемкость выполнения проекта		260

Продолжительность рабочего дня равна 8 часам. Далее делим трудоемкость проекта на продолжительность рабочего дня. В результате для реализации системы защита необходимо 32 рабочих дней. 260:8=32

3.2 Расчет затрат на проектирование системы

Ниже определены затраты для построения и внедрения системы защиты организаций на основе имеющейся сметы, которая включает следующие элементы:

– материальные затраты;
– затраты на оплату труда;
– социальный налог;
– амортизация основных фондов;
– затраты на оборудование и ПО.

Материальные затраты приведены в таблице 3.2.

Таблица 3.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Бумага для офиса	Double A	Упаковка	1	1 950,00	1950,00
Тетрадь (96 листов)	Fruit time	Штук	3	250,00	750,00
Блокнот	Realman	Штук	3	435,00	1305,00
Ручки	Scotland	Штук	4	100,00	400,00
Компьютерная мышь	Crown	Штук	2	5 000,00	10000,00
Итого:					14405,00

Lenovo IdeaPad-SMB V110-15IAP будет использоваться для построения и внедрение системы защиты, характеристики ноутбука хватает для реализаций проекта.

Общую сумму, необходимую на материальные средства ($З_м$) можно рассчитать по следующей формуле:

$$З_м = \sum P_i * Ц_i, \quad (3.1)$$

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.

Расчет затрат на необходимое оборудование и программное обеспечение производится по форме, приведенной в таблице 3.3.

Таблица 3.3 – Расчет затрат на оборудование и ПО, необходимого для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	Lenovo IdeaPad-SMB V110-15IAP	Штук	1	100 000,00	100 000,00
Принтер	Epson Expression Home XP-352	Штук	1	42 599,00	42 599,00
Итого:					142 599,00

Зм = 14 405 + 142 599 = 157 004 (тг)

Для реализации программного обеспечения необходимы материалы на сумму 157 004 тенге.

3.3 Расчет затрат на электроэнергию

При построении и внедрении системы защиты организаций не обойтись без потребления электроэнергии, имеет смысл произвести расчет затрат на электроэнергию.

Для построения и внедрение системы защиты необходимо порядка 260 часов, теперь необходимо рассчитать стоимость электроэнергии, которая будет потрачена в течении 260 часов.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (3.2)$$

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

$З_{доп.нужды.}$ – затраты электроэнергии на дополнительные нужды.

Расчет электроэнергии, которая необходима для оборудования определяется по следующей формуле:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (3.3)$$

где W – потребляемая мощность, Вт;

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

T – время работы;

S – тариф (1кВт/ч = 18,32 тг).

Итоги по расчетам стоимости затрачиваемой электроэнергии представлены в таблице 3.4.

Таблица 3.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/кВтч	Сумма, тг.
Ноутбук	0,6	0,7	260	18,32	2000,54
Модем	0,08	0,9	260	18,32	342,95
Принтер	0,5	0,9	18	18,32	148,39
Кондиционер	0,8	0,9	180	18,32	2374,27
Освещение	0,3	0,7	260	18,32	1000,27
Итого:					5866,42

$$З_{эл.эн.обор.} = 5\,866{,}42 \text{ (тенге)}$$

На дополнительные потребности расходы подсчитываются на основе повышенного показателя в объеме 5% от расходов на электроэнергию:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (3.4)$$

Определим затраты на дополнительные потребности согласно формуле (4.4):

$$З_{доп.нужды} = 0.05 * 5866{,}42 = 293{,}32 \text{ (тенге)}$$

Исходя из всех расчетов, полные расходы на электроэнергию составляют:

$$Э = 239{,}32 + 5\,866{,}42 = 6\,105{,}74 \text{ (тенге)}$$

3.4 Расчет затрат на оплату труда

Для построения и внедрения системы защиты нужны два работника:

− руководитель проекта;

− помощник руководителя проекта.

Сумму расходов на оплату труда можно рассчитать по следующей формуле:

$$З_{тр} = \sum ЧС_i * T_i \quad (3.5)$$

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

T_i - трудоемкость разработки модели, чел.×ч; i - категория работника;

n - количество работников, занятых разработкой ПП.

Во время реализации проекта рабочее время участников не равномерно, поэтому имеет смысл установить часовую ставку каждого работника и общий объем заработной платы.

Часовую ставку сотрудника можно рассчитать по следующей формуле:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (3.6)$$

где $ЗП_i$ - месячная заработная плата i-го работника, тг;

$ФРВ_i$ - месячный фонд рабочего времени i-го работника, час.

Месячная заработная плата сотрудников:

Руководитель проекта – 178 000 тг;

Помощник руководителя проекта – 142 000 тг;

Рабочие часы в день составляют 8 часов, а рабочих дней в месяц составляют 22 дня после вычета выходных 2 дней.

Рассчитаем часовую ставку каждого работника согласно формуле (3.6):

$$ЧС_{руководитель} = \frac{178\,000}{22 * 8} = 1011{,}36 \text{ тг/ч}$$

$$ЧС_{проектировщик} = \frac{142\,000}{22 * 8} = 806{,}8 \text{ тг/ч}$$

Часовая ставка руководителя составляет 1011,31 (тг/ч), трудоемкость руководителя равняется 105 часам (1 этап = 15, 2 этап = 30, 7 этап = 35, 8 этап = 25). Часовая ставка проектировщика составляет 806,8 (тг/ч), трудоемкость помощника руководителя равняется 155 часам (3 этап = 40, 4 этап = 30, 5 этап = 50, 6 этап = 35). Согласно формуле (4.5) можно рассчитать сумму расходов на заработную плату работников:

$$З_{тр} = 1011{,}36 * 105 + 806{,}8 * 155 = 106\,187{,}55 + 125\,054 = 231\,241{,}55$$

Расчеты затрат по оплате труда показаны в таблице 3.5.

Таблица 3.5. – Расчет заработной платы

Категория работника	Квалификация	Трудоемкость проекта, час.	Часовая ставка, тг/ч	Сумма, тг
Руководитель проекта	Инженер-проектировщик	105	1011,36	106 187,55
Помощник руководителя	Инженер-программист	155	806,8	125 054
Итого:				231 241,55

3.5 Расчет затрат по социальному налогу

Согласно Налоговому кодексу Республики Казахстан социальный налог составляет 11% от фонда оплаты труда. Социальный налог можно рассчитать по следующей формуле:

$$С_н = (ФОТ - ПО) * 0,11 \quad (3.7)$$

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

$$ПО = 231\,241,55 * 0,1 = 23\,124,15 \text{ тенге}$$

$$С_н = (231\,241,55 - 23\,124,15) * 0,11 = 22\,892,91 \text{ тенге}$$

Результаты расчетов представлены в таблице 3.6:

Таблица 3.6 – Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель	1	106 187,55	10 618,75	10 512,56
Проектировщик	1	125 054	12 505,4	12 380,35
Итого:				*22*892,91

3.6 Амортизация основных фондов и прочие затраты

Нормы амортизации ОФ необходимо определить в соответствии с налоговым кодексом РК. Амортизацию ОФ можно определить по следующей формуле:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (3.8)$$

где, $С_{об}$ – стоимость оборудования;

$Н_а$ – норма амортизации (норма амортизация = 25);

Формула (4.8) позволяет рассчитать нужную сумму для амортизационных отчислений за год для ноутбука:

$$A_г = \frac{100\,000 * 25}{100} = 25\,000 \text{ тенге}$$

Теперь необходимо рассчитать норму амортизации за период проектирования:

$$A_г = \frac{25000 * 32}{365} = 2\,191,7 \text{ тенге}$$

Подобным образом необходимо рассчитать норму амортизации для всего оборудования. Результаты расчетов приведены в таблице 3.7.

Таблица 3.7 – Амортизация ОФ

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время проектирования, тг
Ноутбук	100 000	25	25 000	2 191,7
Принтер	42 599	25	10 649	933,61
Итого:			35 649	3 125,31

На основе всех представленных расчетов необходимо оформить смету расходов на проектирование системы защиты согласно форме, которая приведена в таблице 3.8 (рисунок 13).

Таблица 3.8 – Смета затрат на проектирование системы защиты

Статьи затрат	Сумма, тг	Проценты, %
Затраты на материальные ресурсы	14 405,00	4
Затраты на оборудование и ПО	157 004	42
Затраты на оплату труда	231 241,55	46
Социальные налоги	22 892,91	5
Затраты на электроэнергию	6 105,74	2
Амортизация основных фондов	3 125,31	1
Итого по смете:	434 774,51	100

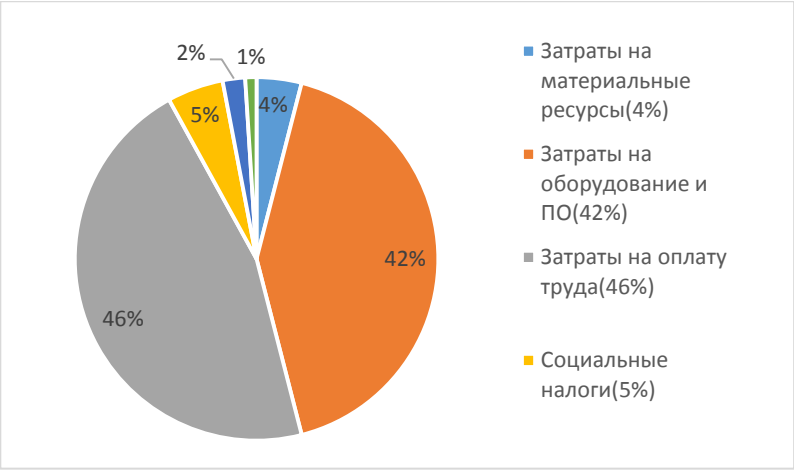

Рисунок 13 – Диаграмма затрат

3.7 Определение возможной (договорной) цены системы защиты

Стоимость системы защиты определяется на основе качества разработанной системы, сроков его проектирования и производительности. Стоимость $Ц_Д$ для системы защиты можно рассчитать по следующей формуле:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (3.9)$$

где $З_{нир}$ – затраты на проектирование системы защиты, тг;

Р – средний уровень рентабельности, (%). Данный параметр принят равным 25%.

$$Ц_Д = 434\,774{,}51\left(1 + \frac{25}{100}\right) = 434\,774{,}51 + 108\,693{,}63 = 543\,468{,}2 \text{ тенге}$$

Далее необходимо определить стоимость реализации с учетом НДС, ставка НДС устанавливается законодательством РК. На 2019 года ставка НДС составляет 12%. Стоимость реализации учитывая НДС можно рассчитать по следующей формуле:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (3.10)$$

$$Ц_р = 543\,468{,}2 + 543\,468{,}2 * 0{,}12 = 608\,684{,}38 \text{ тенге}$$

3.8 Вывод по экономическому разделу

Себестоимость = 434 774,51тенге
Прибыль = 108 693,63 тенге
Цена реализации с учетом НДС = 608 684,38 тенге

4 Безопасность жизнедеятельности

4.1 Анализ условия труда при работе в офисным помещений

Помещение, в котором исследуется освещение, представляет собой одну комнату, где работают 4 человека, со следующими параметрами: длина L = 4 м, ширина B = 3м, высота H = 3 м. В помещении имеется оконный проем длиной 3 м и высотой 2 м. В офисе имеется четыря рабочих места с современными компьютерами мощностью 230 Вт. План помещения представлен на рисунке 1.

Учитывая род деятельности сотрудников, а в нашем случае это постоянная работа с персональным компьютером, конструкция рабочего стола обеспечивает оптимальное размещение на рабочей поверхности используемого оборудования с учётом его количества и конструктивных особенностей (размер монитора, клавиатуры и других). Конструкция рабочей мебели (столы и кресла) обеспечивает возможность индивидуальной регулировки. Рабочие места, высотой 0,8 м, размещены вертикально к окну.

Характеристики используемого оборудования.

Модель системы создается и запускается на ноутбуке, сборка и припаивание элементов платы на паяльной станции, происходит в отдельной комнате на обычном столе. В помещении имеются 2 ноутбука и паяльная станция:

а) Рабочая станция 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.

Данное оборудование не обладает сильным шумовым воздействием. Вероятность возгорания рабочий станций или поражение током - мала, а для предотвращения пожара достаточно установленного огнетушителя

Соблюдены следующие основные условия:

– оптимальное размещение оборудования, входящего в состав рабочего места;

– достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения;

– уровень акустического шума не превышает допустимого значения.

Единственной проблемой, которая препятствует для повышения уровня труда в помещении с параметрами L:B:H=4:3:3, я думаю, является недостаток освещения. Данное помещение имеет одно окно с площадью равной S=6м2 и один светильник типа ЛПО 12-2×40-904..

Исходя из этих факторов, я решил произвести расчет естественного и искусственного освещения данного офисного помещения.

В производственных помещениях используется три вида освещения:

– естественное (источником его является солнце);

– искусственное (использование только искусственных источников света);

– совмещенное, или смешанное (сочетание естественного и искусственного освещения).

Естественное освещение создается природными источниками света – прямыми солнечными лучами и диффузным светом небосвода (от солнечных лучей, рассеянных атмосферой). Естественное освещение является биологически наиболее ценным видом освещения, к которому максимально приспособлен глаз человека.

В производственных помещениях используются следующие виды естественного освещения:

– боковое – через светопроемы (окна) в наружных стенах;

– верхнее – через световые фонари в перекрытиях;

– комбинированное – через световые фонари и окна.

Искусственное освещение на промышленных предприятиях осуществляется лампами накаливания и газоразрядными лампами, которые являются источниками искусственного света.

В зданиях с недостаточным естественным освещением применяют совмещенное освещение – сочетание естественного и искусственного света. Искусственное освещение в системе совмещенного освещения может функционировать постоянно (в зонах с недостаточным естественным освещением) или включаться с наступлением сумерек.

В помещении применяется естественное и искусственно освещение. Естественное освещение осуществляется через окно, показанным на плане помещения. Для защиты от избыточного света и ярких лучей используются регулируемые жалюзи с вертикальными ламелями (рисунок 14).

Существующая схема расположение светильников

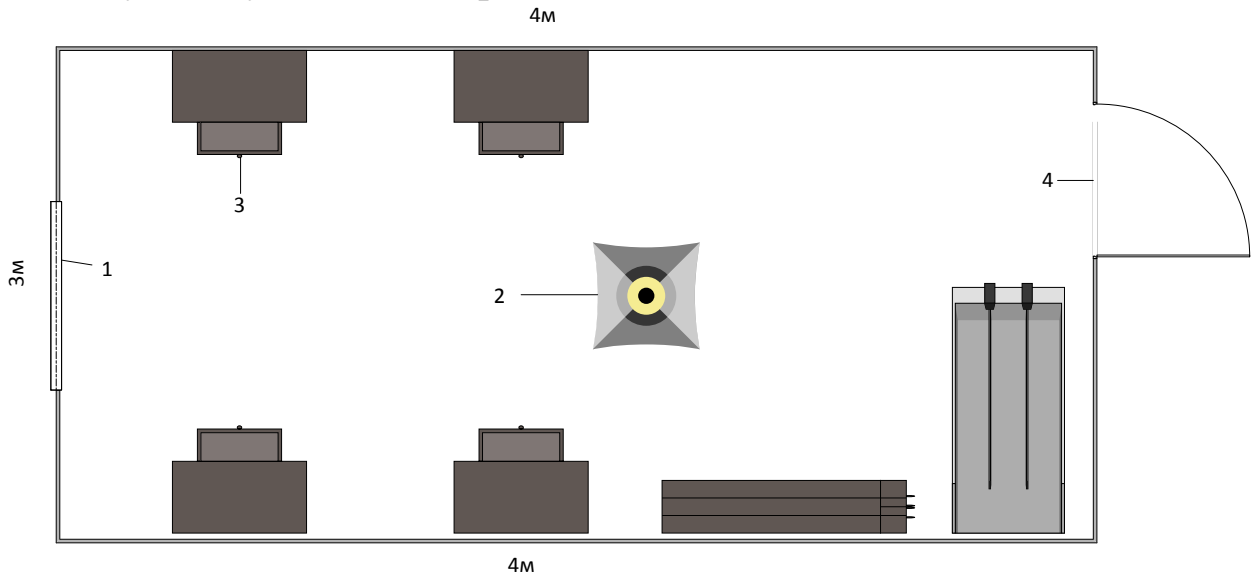

Рисунок 14 – План помещения

1 – оконной проем, 2 – светильник 3 – рабочее место, 4 – дверной проем.

Условие задачи

Рассчитать необходимую площадь окна для создания нормируемой естественной освещенности в производственном помещении.

Исходные данные

Помещение: офисное помещение

Габариты (L x B x H) 4 x 3 x 3

Количество светильников: 1

Тип светильников: ЛПО 12-2×40-904 (производство PHILIPS)

Разряд зрительной работы: I, б

Коэффициент отражения: Рпот=70%, Рст=50%, Рпол=30%

4.2 Расчетная естественного освещения

Изначально в помещение в котором мы рассматривали было 1 лампа и окно 6м2

Площадь боковых проемов при боковом освещении определяется из следующей формулы:

$$100 * \frac{S_0}{S_n} = \frac{e_N \times K_з \times \eta_0}{\tau_0 \times \tau_1} \times К_{зд},$$

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

S_n – площадь пола помещения, м2;

e_N – нормируемое значение КЕО;

$К_З$ –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;

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

Определим площадь пола помещения:

$$S_n = L \cdot B$$

$$S_n = 4 \cdot 3 = 12 \text{ м}^2$$

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

$$e_N = e_H \cdot m_N$$

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 I а разряд зрительных работ, найдем:

$e_H = 2.0$

Следовательно:

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

Учитывая тип помещения, найдем коэффициент запаса.

$К_з$=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 $\frac{l}{h_{расч}}$.

$$l = 3 - 1 = 2 \text{ м}$$

$$\frac{L}{l} = \frac{4}{2} = 2$$

Найдем $h_{расч}$:

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

$h_{расч}$=3-0,5-0,8=1,7 м;

$$\frac{l}{h_{pac}} = \frac{2}{1.7} = 1.17 \approx 1.2$$

$$\frac{l}{B} = \frac{2}{3} = 0.6 \approx 1$$

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:

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

$$\rho_{ср} = \frac{\rho_{пот}\rho_{стен}\rho_{пол}}{3}\% = \frac{70+50+30}{3} \approx 0{,}5$$

r_l=1,7

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

$$\frac{Р}{Н_{зд}} = \frac{10}{18} = 0.55 => К_{зд} = 1.7$$

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

$$S_0 = \frac{S_n \cdot e_N \cdot К_з \cdot \eta_0}{100 \cdot \tau_0 \cdot r_1} \cdot К_{зд}$$

$$S_0 = \frac{12 \cdot 1.3 \cdot 1.2 \cdot 8{,}5 \cdot 1{,}7}{100 \cdot 0.64 \cdot 1{,}7} \approx 2.5 \text{ м}^2$$

Таким образом данных рассчетов ествественное освещение удовлетворяет рассчитаному нормативному значения, но надо произвести расчет искуственого помещения, так как сотрудники работают в вечерние время тоже.

4.3 Расчет искусственного освещения

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.

$$Е_\tau = \frac{N*n*ф*\mu}{K*S*z} = \frac{1*1*2850*0{,}45}{1.5*12*1.1} \approx 64.1 лк$$

Получилась у нас 64.1 < 300 что не удовлетворяет условному значению.

Фактическая освещенность $Е_\tau$ производственного помещения получилось меньше нормативной освещенности $Е_н$, поэтому производим реконструкцию помещения, тем самим увеличивая количество светильников в омещения.

Определение расчетной высоты подвеса:

$$h_{расч} = H_{помещения} - Н_{свеса} - Н_{р.п.},$$

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.

$$h_{расч}=3-0,5-0,8=1,7 \text{ м};$$

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

Индекс помещения определяется по формуле :

$$i = \frac{A * B}{h_{расч} * (A + B)} = \frac{3 * 4}{1,7(3 + 4)} = \frac{12}{11,9} = 1,008$$

где А- длина помещения , м;

В- ширина помещения , м;

$h_{расч}$ - расчетная высота, м.

По таблице 15 для светильника типа TLPL228.2x36 находим η = 0,55.

Таким образом, количество светильников равно:

$$N = \frac{E_т \cdot K_З \cdot S \cdot z}{n\ ф \cdot \mu} = \frac{300 \cdot 1.2 \cdot 12 \cdot 1.1}{1 * 2850 * 0,45} \approx 4$$

$E_н$ = 300 лк - заданное номинальное освещение.

S = 12м^2 – площадь помещения.

z = 1,1- коэффициент неравномерности освещения.

n- количество ламп в светильнике.

ф = 2850 лм

$$N = \frac{200 * 1,5 * 242 * 1,1}{0.44 * 2 * 3120} N \approx 4 \text{шт}$$

Определим необходимое расстояние между светильниками по формуле:

$$L = \lambda * h;$$

где L – Расстояние между соседними светильниками;

h – Высота подвеса светильника над рабочей поверхностью.

Таким образом, необходимое расстояние между светильниками:

$$L = 0.8 * 1.7 \approx 1,3 \text{м}$$

Расстояние между рядами светильников:

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

Расстояние между светильником и стеной:

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

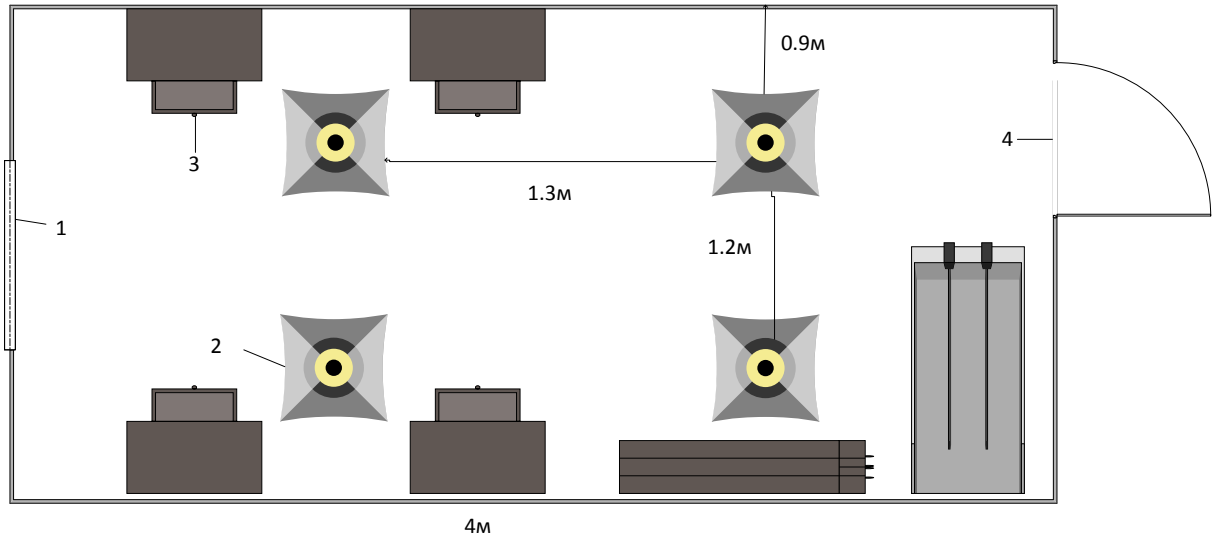

Рисунок 15 – План помещения (после реконструкций)

4.4 Вывод по разделу безопасность жизнедеятельности

В разделе БЖД был проведен расчет естественного освещения. При проверки естественного освещения помещений необходимо определить площадь световых проемов, обеспечивающих нормированное значение КЕО. В офисном помещение для обеспечения нормированного значения КЕО, eN= 1.3, при разряде I, б окна 6м2 обеспечивает нормирования значение зрительных работ требуется площадь световых проемов равная 2.5м2 (рисунок 15).

Далее был проведен расчет искусственного освещения. Расчет освещенности по коэффициенту использования светового потока показал, что заданного числа светильников было меньше необходимого для обеспечения достаточной освещенности помещения. Для обеспечения необходимой освещенности помещения необходимо увеличить количество светильников до 4 штук, чтобы обеспечить нормальное освещения для человеческого глаза.

Заключение

Современной организаций характерна информационная система с присущими ей процессами сбора, обработки, хранения, накопления информации. В данных процессах используется информация разного уровня доступа и функционального применения, которая может подвергаться воздействию различных видов угроз. И в настоящее время в связи с активным развитием информационных технологий в производственных предприятиях возрастает количество проблем, связанных с ИБ.

В дипломной работе выполнен анализ и было проведено теоретическое обобщение известных средств, технологий и методов защиты конфиденциальной информации применительно к ТОО «PC4U».

В силу Закона Республики Казахстан «Об информатизации», Закона Республики Казахстан «О персональных данных и их защите» необходимо принимать меры по защите персональных данных от разглашения, меры защиты электронных информационных ресурсов, а также использовать системы контроля доступа и регистрации фактов доступа к информации. В качестве оптимального метода защиты информации, по вышеуказанным требованиям, в условиях решения задач ИБ была выбрана DLP-система на основе аппаратно-программного решения «Инспектор».

АПК «Инспектор» является отечественным продуктом и эффективным методом защиты информационных ресурсов и ИС в целом. Данная система обеспечивает:

- целостность данных;
- значительное снижение рисков утечки ценной информации;
- возможность предупредить утечку конфиденциальной информации;
- снижение рисков, связанных с халатностью и безграмотностью пользователей компьютеров;
- интегрирование с устройствами сторонних производителей;
- увеличение роста производительности сотрудников.

При написании дипломной работы выполнены все поставленные задачи:

- проведен системный анализ уязвимости системы обеспечения информационной безопасности организаций;
- изучена общая структура образовательной информационной системы;
- определены потенциальные источники угроз и уязвимые места;
- изучены и проведен сравнительный анализ современных методов и систем защиты информации;
- обосновано внедрение метода защиты ИС;
- внедрен АПК «Инспектор» в ТОО «PC4U»;
- приведены конкретные предложения и рекомендации по защите ИС ТОО «PC4U»;
- разработана концепция информационной безопасности организаций;
- разработана политики информационной безопасности организаций.

В рамках данной дипломной работы была проанализирована актуальная проблема защиты от утечки информации конфиденциального характера и ограниченного доступа в информационной среде ТОО «PC4U», что требует внедрения новых программно-технических решений. Приведены необходимые статистические данные и параметры, основные функциональные возможности АПК «Инспектор», порядок и способы установки и настройки аппаратно-программного обеспечения.

Раскрыты особенности DLP-технологии как основного инструмента защиты от утечки информации, способы установки клиентской части (агентов) АПК на персональные компьютеры: вручную, с помощью программного обеспечения Active Directory. В работе приведены структурно-функциональная схема работы АПК «Инспектор», основной алгоритм ее работы и необходимые результаты анализа эффективности работы системы, полученные после ее запуска в пилотном режиме на основе экспериментальных отчетов.

Оценка эффективности обеспечения ИБ ИС с использованием аппаратно-программного решения на базе ТОО «PC4U» и определение степени правильности реагирования системы на нарушения требований ИБ были осуществлены экспериментально. Были анализированы нарушения правил безопасности сотрудниками с использованием 15 рабочих станций.

В результате анализа ИС ТОО «PC4U» было выявлено несколько нарушений работы сотрудников с ПК, с рабочими файлами и документами, программами и прочими интернет-ресурсами. После выявлений нарушений с помощью системы мониторинга и контроля действий «Инспектор» были приняты определенные меры.

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%.

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

В рамках данной дипломной работы был запущен пилотный режим АПК «Инспектор», в дальнейшем данная система будет работать. Будут выполнены более глобальные настройки и подготовлены все необходимые документы. С помощью данной системы, оценивая все информационные потоки, как люди работают с документами и файлами, можно классифицировать все данные по степени конфиденциальности и вносить изменения в саму программу: создавать папки, вносить дополнительные настройки, создать более удобный интерфейс.

Таким образом, внедрение системы АПК «Инспектор» позволило решить задачу блокирования утечки информации ограниченного доступа через каналы связи в инфраструктуре ТОО «PC4U». Возможности системы также позволило определить структурную часть – источник и канал утечки, которая в дальнейшем устранит всякие попытки утечек и хищения информационных ресурсов. Из вышеизложенного можно прийти к выводу, что выбор и внедрение в информационную систему аппаратно-программного решения «Инспектор» позволит обеспечить решение задач ИБ на вполне эффективном уровне.

Список литературы

1 Усков А.В., Иванников А.Д., Усков В.Л. Educational Technology & Society 11(1) Технологии обеспечения информационной безопасности корпоративных образовательных сетей 'Государственный научно-исследовательский институт информационных технологий и телекоммуникаций «Информика», –М:. ISSN 1436-4522,2008 г.

2 Проталинский О.М., Ажмухамедов И. М. Информационная безопасность вуза, Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ., 2009, № 1, 18–23.

3 Волков А.В. Обеспечение ИБ в вузе. Журнал "Information Security/ Информационная безопасность" 2006 г. - № 3, 4.

4 Шемяков А.О. Научно-методический аппарат оценки уязвимости системы обеспечения безопасности информации в современном вузе. – Серпухов: РГБ ОД, 2013.- 130 с.

5 Мясоедова Е.А., Будникова Г.А. Информационная образовательная среда учреждения: понятие, структура, проектирование. Астраханский институт повышения квалификации и переподготовки. Народное образование. Педагогика. № 2. УДК 37.2012 г. - 9 с.

6 Захарова И.Г. Информатизационные технологии в образовании: Учеб. пособие для студ. высш. пед. учеб. заведений. – М.: Издат. центр «Академия», 2003. – 58 с.

7 КубеевЕ.К., Каргин С.Т. Учебный процесс в КарГУ. –Караганда: КарГУ, 2003. – 9 с.

8 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.

9 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

10 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.: ил. – (Профессиональное образование).

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

12 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".

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.

Перечень сокращений

ARP – Address Resolution Protocol, Протокол разрешения адресов
BGP – Border Gateway Protocol, Протокол граничных шлюзов
DNS – Domain Name System, Доменная система имен
DoS – Denial of Service, Отказ в обслуживании
FTP File Transfer Protocol, Протокол передачи файлов
HTTP – Hypertext Transfer Protocol, Протокол передачи гипертекстовой информации
IP – Internet Protocol, Межсетевой протокол
IT – Information technology, Информационные технологии
MAC – Media Access Control, Управление доступом к среде передачи
NAT – Network Address Translation, Трансляция сетевых адресов
OSI – Open System Interconnection, Взаимодействие открытых систем
SSL – Secure Sockets Layer, Уровень безопасных соединений
SSH – Secure Shell, Безопасная оболочка
TCP – Transmission Control Protocol, Протокол управления передачей
UDP – User Datagram Protocol, Пользовательский датаграмный протокол
URL – Uniform Resource Locator, Унифицированный определитель местонахождения
VoIP – Voice over IP, Передача голоса по интернет-протоколу
VPN – Virtual Private Network, Виртуальные частные сети
VLAN –Virtual Local Area Network, Виртуальная локальная вычислительная сеть
WWW – World Wide Web, Распределенная всемирная сеть
IDS – Intrusion Detection System, Система обнаружения вторжений
СОВ – Система обнаружения вторжений
IMAP – Internet Message Access Protocol, Протокол прикладного уровня для доступа к электронной почте
POP – Post Office Protocol, Протокол почтового отделения
GC – Global Catalogue, Глобальный каталог
HIPS – Host-based Intrusion Prevention System, система предотвращения вторжений
АПК – Аппаратно-программный комплекс
ИБ – Информационная безопасность
ИС – Информационная система
ИКТ – Информационно-телекоммуникационные технологии
ПК – Персональный компьютер
ЗИ – Защита информации
ИБ – Информационная безопасность