Министерство образования и науки Республики Саха (Якутия)
Государственное автономное профессиональное образовательное учреждение Республики Саха (Якутия)
«Региональный технический колледж в г. Мирном»

Специальность 09.02.02
«Компьютерные сети»
группа КС 16/9

КУРСОВОЙ ПРОЕКТ

Тема работы: **«Обеспечение безопасности компьютерной сети на базе рекламного агентства «Deltaplan» »**

Студент: Чащина Александра Андреевна
(подпись) (Фамилия, Имя, Отчество)

Руководитель проекта: Володькин Евгений Владимирович
(подпись) (Фамилия, Имя, Отчество)

Работа допущена к защите с оценкой
(дата)

Зам. директора по УР: Мусорина Алиса Александровна
(подпись) (расшифровка) (дата)

Мирный 2020

ЗАДАНИЕ НА КУРСОВОЕ ПРОЕКТИРОВАНИЕ

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5

1 ОСНОВНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ 8

1.1 Описание объекта защиты и существующей в нем компьютерной сети 9

1.2 Обзор и анализ существующих угроз безопасности компьютерной сети 11

1.3 Анализ средств защиты информации 14

2 РАЗРАБОТКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КС НА БАЗЕ РЕКЛАМНОГО АГЕНСТВА «DELTAPLAN» 16

2.1 Обеспечение информационной безопасности 17

2.2 Управление доступом к информации 18

2.3 Защита информации программными средствами 20

2.4 Физическая защита информации 21

2.5 Разработка системы контроля и управления доступом 21

2.6 Разработка подсистемы видеонаблюдения 26

3 ЭКОНОМИЧЕСКИЙ РАСЧЕТ 29

ЗАКЛЮЧЕНИЕ 34

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 37

ПРИЛОЖЕНИЕ А 39

ПРИЛОЖЕНИЕ Б 41

ВВЕДЕНИЕ

					РТК.О. 09.02.02 02 КС-16/9 ПЗ			
Изм.	Лист	№ докум	Подпись	Дата				
Выполнил		Чащина А.А.			ВВЕДЕНИЕ	Литера.	Лист	Листов
Руководит.						У	5	3
Рецензент		Володькин Е.В				ГАПОУ РС(Я) «МРТК»		
Н. контр.								
Утвержд		Мусорина А.А						

ВВЕДЕНИЕ

Обеспечение информационной безопасности на сегодняшний день названо первой из пяти главных проблем локальных сетей и сети Internet, которая представляет собой эффективную, но вместе с тем и непредсказуемую среду, полную разнообразных угроз и опасностей.

Под **сетевой безопасностью** принято понимать защиту информационной инфраструктуры объекта (при помощи аутентификации, авторизации, межсетевых экранов, систем обнаружения вторжений IDS/IPS и других методов) от вторжений злоумышленников извне, а также защиту от случайных ошибок (с применением технологий DLP) или намеренных действий персонала, имеющего доступ к информациям внутри самого предприятия.

Актуальность работы состоит в:

1. Появление новых информационных технологий;
2. Сосредоточение в единых базах информации различного назначения и различной принадлежности;
3. Расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
4. Бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
5. Повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;
6. Развитие глобальной сети Internet, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире;

Эти проблемы вызвали необходимость в том, чтобы *эффективность защиты информации росла вместе со сложностью архитектуры хранения данных.*

Цель курсового проекта – разработка обеспечения системы безопасности компьютерной сети рекламного агентства "DELTAPLAN".

Для достижения поставленной цели были поставлены следующие **задачи:**

- выявить и оценить угрозы характерные для локальных сетей;
- выбрать программные средства для обеспечения безопасности ЛВС;

- рассмотреть и подобрать физические средства защиты информации;
- разработать систему контроля и управления доступа;
- разработать подсистему видеонаблюдения.

Объектом проектирования является работоспособная сегментированная компьютерная сеть.

Предметом проектирования являются методы обеспечения безопасности компьютерной сети.

ОСНОВНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

					РТК.О. 09.02.02 02 КС-16/9 ПЗ			
Изм.	Лист	№ докум	Подпись	Дата				
Выполнил		Чащина А.А.			ОСНОВНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ	Литера.	Лист	Листов
Руководит.						У	8	7
Рецензент		Володькин Е.В				ГАПОУ РС(Я) «МРТК»		
Н. контр.								
Утвержд		Мусорина А.А						

1 ОСНОВНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

1.1 Описание объекта защиты и существующей в нем компьютерной сети

В данной курсовой работе рассматривается информационная инфраструктура рекламного агентства "DELTAPLAN".

Офис рекламного агентства находится в девятиэтажном здании бизнес-центра на четвертом этаже. План здания представлен в приложении А.

1. Каб.401 «Пост Охраны» (2 ПК, один с системой СКУД, 1 ИБП, 2 монитора видеонаблюдения);
2. Каб.402 «Гардероб»;
3. Каб.403 «ИВО» (7 ПК, 1 МФУ, 1 ИБП);
4. Каб.404 «Серверная» (2 ИБП, 3 сервера, 1 коммутатор, мини АТС);
5. Каб.405 «ОК» (3 ПК, 1 МФУ, 1 ИБП);
6. Каб.406 «Отдел Творческих разработок» (7 ПК, 1 плоттер, 1 ИБП, 1 МФУ);
7. Каб.407 «Актовый зал» (Акустические и конгресс-системы, интерактивные панели, PTZ камеры, системы видеоконференцсвязи, отображения информации с мобильных устройств, управления оборудованием);
8. Каб.408 «Отдел по работе с клиентами» (4 ПК, 1 МФУ);
9. Каб.409 «Приемная» (1 ПК, 1 МФУ, 1 ИБП);
10. Каб.410 «Директор» (1 ПК, 1 принтер);
11. Каб.411 «Зам. Директора» (1 ПК, 1 принтер);
12. Каб.412«Бухгалтерия» (4 ПК, 1 ИБП, 1 МФУ);
13. Каб.413 «Глав. Бухгалтер» (1 ПК, 1 ИБП, 1 МФУ);
14. Отдел «Отдел медиа-планирования» (18 ПК, 1 МФУ);
15. Отдел «Внутренне-обеспечивающий отдел» (14 ПК, 1 МФУ).

Проектирование требуемой системы защиты информации начинается с системного анализа существующей системы защиты информации, который включает:

1. Моделирование объекта защиты:

- Определение источников защищаемой информации (люди, документы, физические поля, материальные объекты);
- Описание пространственного расположения основных мест расположения источников защищаемой информации.

2. Моделирование угроз безопасности информации:

- Моделирование физического проникновения злоумышленника к источникам информации;
- Моделирование технических каналов утечки.

Для создания полной модели объекта защиты необходимо для начала определить ту информацию, которую необходимо защищать, поэтому необходимо провести её структурирование.

Структурирование информации производится путем классификации информации в соответствии с функциями, задачами и структурой организации с привязкой элементов информации к её источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Моделирование состоит в анализе на основе пространственных моделей возможных путей распространения информации за пределы контролируемой зоны.

Моделирование объекта защиты начинается с построения **структурной модели:**

Таблица 1.1.1 - Структурная модель объекта защиты

№	Наименование элемента информации	Гриф конфиденциальности	Ценность инф-ии %	Наименование источника информации	Местонахождение источника информации
1	Личные сведения о сотрудниках фирмы	Конфиденциально	100	Контракты и электронные документы	Компьютер и шкаф в приемной
2	Сведения о заработной плате работников	Конфиденциально	100	Электронные и бумажные документы	Компьютеры и сейф в бухгалтерии

Продолжение таблицы 1.1.1

3	Данные о сотрудниках отдела	Конфиденциально	10	Контракты и электронные документы	БД на электронных носителях
4	Экономические прогнозы	Конфиденциально	50	Работники отдела логистики, бум, и ком. документы	Компьютеры, документы в отделе логистики
5	Сведения о результатах закупок	Конфиденциально	70	Бухгалтеры, электронные и бумажные документы	Компьютеры и сейф в бухгалтерии
6	Сведения о финансовых операциях	строго конфиденциально.	100	Бухгалтеры, электронные и бумажные документы	Компьютеры и сейф в бухгалтерии

Из приведенной выше таблице видно, что в основном это бумажные и электронные документы.

Таким образом, было проведена классификация и структурирование информации в соответствии с функциями, задачами и структурой организации, в результате чего защищаемая информация была представлена в виде отдельных элементов информации.

Всего к сети подключено 64 рабочих станций. К каждому рабочему месту подведены IP-телефоны. В целях безопасности установлены видеонаблюдение с помощью IP камер. Используется топология звезда, с архитектурой FastEthernet, по стандарту 100BASE-TX, обеспечивающий передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из витой пары 5 категории. Длина линии связи ограничена 100 метрами, но по одному стандартному кабелю, имеющему 4 пары, при необходимости можно организовать два 100-мегабитных канала связи. В девяти кабинетах имеется многофункциональное устройство (устройство, сочетающее в себе функции принтера, сканера, факсимильного устройства, копировального модуля) оно подключено с помощью прямой локальной сети между рабочими местами в кабинете. В каждом кабинете имеется источник бесперебойного питания. Схема подключения устройств представлена в приложении Б.

1.2 Обзор и анализ существующих угроз безопасности КС

Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.

Угрозы безопасности информационных систем классифицируются по нескольким признакам (1.3.1).

К **естественным** относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д.

Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными.

Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации.

Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации.

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциалной информации. При реализации этих угроз *информация* становится известной лицам, которые не должны иметь к ней *доступ*. Несанкционированный *доступ* к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, *копирование* этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством *сети передачи данных*, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации.

Рисунок. 1.2.1 Классификация угроз безопасности информационных систем

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют *доступ* к некоторым её ресурсам.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию.

Под **внешними угрозами** безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды.

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

1 Нежелательный контент.

2 Несанкционированный доступ.

3 Утечки информации.

4 Потеря данных.

5 Мошенничество.

6 Кибервойны.

7 Кибертерроризм.

1.3 Анализ средств защиты информации

Защита информации представляет собой деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных (случайных) воздействий на защищаемую информацию.

Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае.

- Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно:

1. использовать качественные комплектующие,
2. проводить регулярное техническое обслуживание,
3. устанавливать стабилизаторы напряжения.

- Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО).
- Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно.
- Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасного программного обеспечения на компьютер.
- Также в качестве меры предосторожности от потери информации следует делать резервные копии.
- Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий:

1 защита от нежелательного контента (антивирус, антиспам, веб-фильтры,

анти-шпионы);

2 сетевые экраны и системы обнаружения вторжений (IPS);

3 управление учетными данными (IDM);

4 контроль привилегированных пользователей (PUM);

5 защита от DDoS;

6 защита веб-приложений (WAF);

7 анализ исходного кода;

8 антифрод;

9 защита от таргетированных атак;

10 управление событиями безопасности (SIEM);

11 системы обнаружения аномального поведения пользователей (UEBA);

12 защита АСУ ТП;

13 защита от утечек данных (DLP);

14 шифрование;

15 защита мобильных устройств;

16 резервное копирование;

17 системы отказоустойчивости.

РАЗРАБОТКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КС НА БАЗЕ РЕКЛАМНОГО АГЕНСТВА «DELTAPLAN»

					РТК.О. 09.02.02 02 КС-16/9 ПЗ			
Изм.	Лист	№ докум	Подпись	Дата				
Выполнил		Чащина А.А.			РАЗРАБОТКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КС НА БАЗЕ РЕКЛАМНОГО АГЕНСТВА «DELTAPLAN»	Литера.	Лист	Листов
Руководит.						у	16	11
Рецензент		Володькин Е.В				ГАПОУ РС(Я) «МРТК»		
Н. контр.								
Утвержд		Мусорина А.А						

2 РАЗРАБОТКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КС НА БАЗЕ РЕКЛАМНОГО АГЕНСТВА «DELTAPLAN»

2.1 Обеспечение информационной безопасности

Обеспечение информационной безопасности (ИБ) – комплексная задача, решаемая параллельно по целому ряду направлений: *правовому, организационному и техническому*. Эффективное обеспечение ИБ возможно только при создании **системы обеспечения информационной безопасности** (СОИБ), охватывающей все направления деятельности организации и функционирующей на всех уровнях управления (стратегическом, тактическом и оперативном).

СОИБ представляет собой сложную организационно-техническую структуру, состоящую из:

- комплексной системы защиты информации – совокупности интегрированных программно-технических средств защиты информации, обеспечивающих защиту информационных ресурсов во всех информационных системах Заказчика и на всех этапах их жизненного цикла;
- совокупности процессов, обеспечивающего эффективную эксплуатацию и развитие комплексной системы защиты информации;
- персонала – сотрудников подразделений ИБ, занятых в процессах эксплуатации комплексной системы защиты информации, а также контроля над выполнением требований внутренних документов в области ИБ и прочих задачах обеспечения ИБ.

При создании СОИБ мы ориентируемся на ряд ключевых принципов, которым должна отвечать система обеспечения информационной безопасности:

- соответствие мер защиты, реализуемых СОИБ, реальным угрозам ИБ (которые определяются предварительно, по результатам аудита ИБ);
- поэтапное создание СОИБ с целью оптимизации финансовых затрат, сохраняющее при этом единую концепцию СОИБ;
- защита инвестиций – использование существующих средств и систем защиты информации для построения СОИБ, с целью снижения капитальных затрат (в

том числе интеграция разнородных подсистем обеспечения ИБ путем создания единой интегрированной системы);

- централизованное управление и мониторинг, что снижает трудозатраты на эксплуатацию СОИБ;
- учет и эффективная интеграция с существующими процессами управления информационными технологиями.

2.2 Управление доступом к информации

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи, процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).

Речь идет о логическом управлении доступом, который реализуется программными средствами. **Логическое управление доступом** - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и их доступность путем запрещения обслуживания неавторизованных пользователей.

Парольная аутентификация сегодня не способна обеспечить необходимый уровень ИТ-безопасности, о чем свидетельствуют регулярные сообщения об утечках корпоративной информации. Слабые пароли и связанные с ними проблемы продолжают оставаться главными уязвимостями.

Для решения этих проблем используются технологии строгой аутентификации и единого входа. На российском рынке к числу таких систем относится комплекс решений Indeed ID, разработанный компанией `Индид`. Данный комплекс предлагает решения Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On для аутентификации и управления доступом.

Задачи строгой и усиленной аутентификации реализует продукт Indeed Enterprise Authentication которая интегрируется с выбранной системой СКУД для рекламного агентства «DELTAPLAN».

Позволяя заменить парольный доступ на строгую аутентификацию, Indeed Enterprise Authentication освобождает сотрудников от необходимости запоминать и

хранить пароли в секрете, выполнять их регулярную смену согласно парольным политикам безопасности, а также избавляет пользователей от необходимости ручного ввода паролей с клавиатуры.

Вместо ввода пароля в окне аутентификации необходимо просто приложить смарт-карту.

Indeed Enterprise Authentication предоставляет следующие возможности:

- доступ к ресурсам домена Microsoft Active Directory с использованием технологии строгой аутентификации;
- хранение паролей пользователей и их автоматическая смена согласно установленным политикам безопасности;
- опциональная генерация случайных паролей;
- возможность комбинировать все поддерживаемые технологии аутентификации в рамках одной ИТ-инфраструктуры;
- доступ к ресурсам домена из внутренней сети и к службам, доступным из внешней сети (почта, веб-приложения);
- доступ по кэшированному (сохраненному) аутентификатору в случае отсутствия связи с сервером Indeed;
- автоматическая блокировка рабочей станции (например, при извлечении устройства аутентификации или использовании экранной заставки);
- самостоятельная регистрация аутентификаторов и управление ими для пользователей;
- автоматическая идентификация пользователя по аутентификатору без необходимости ввода логина;
- автоматическая подстановка пароля в скрытом виде в нужное поле при нажатии комбинации `горячих клавиш`;
- работа на терминальных серверах Microsoft и Citrix;
- журналирование событий системы Indeed Enterprise Authentication и аудит действий администраторов и пользователей;
- построение отчетов о событиях системы;
- интеграция с системами контроля и управления физическим доступом;

- интеграция с системами управления ключевыми носителями (Card Management System, CMS);
- интеграция с системами управления жизненным циклом и правами учетных записей пользователей (Identity Management, IDM).

2.3 Защита информации программными средствами

Для эффективной защиты информации, обрабатываемой, хранящейся и циркулирующей в локальной сети предприятия используются следующие программные средства:

- Межсетевой экран (Kerio Control);
- Антивирусная программа (ESET NOD32);
- Proxy server (Cool Proxy);
- Сервис защиты от DDoS-атак (Cost of a DDoS attack от Akamai);
- Резервное копирование.

В качестве межсетевого экрана на предприятия используется **KerioControl**, который устанавливается на серверах под управлением Windows. KerioControl - надежный и стабильно работающий межсетевой экран. После его установки и квалифицированной настройки информация находится под надежной защитой, а сотрудники заниматься работой, не отвлекаясь на посторонние ресурсы. Он осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Для защиты компьютерной сети от различных вирусов на предприятии используются **Антивирус ESET NOD32**, он защищает компьютер от вирусов и шпионских программ за счёт применения интеллектуальных технологий ESET. Функция расширенного сканирования памяти помогает заблокировать зашифрованные вредоносные программы, сложные для обнаружения.

CoolProxy - это прокси-приложение, предназначенное для доступа к ресурсам Интернет из сети через соединение с помощью модема или сети. В программе осуществляется кэширование ранее просмотренных страниц, и дает возможность просматривать эти страницы в offline режиме. Приложение CoolProxy дает возможность ограничить рекламу и непроверенные сайты.

Резервное копирование - процесс создания копии данных на носителе (внешнем жестком диске, CD/DVD-диске, флэшке, в облачном хранилище и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

2.4 Физическая защита информации

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов, и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

- охрана территории предприятия и наблюдение за ней;
- охрана здания, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации.

Количество сотрудников в организации - 64 человек из этого можно сделать ряд выводов: система защиты не должна быть громоздкой, должна быть эффективной в рамках средней организации, окупаться в небольшие сроки 3-5 лет. С целью упрощения охраны объекта, в помещениях установлено видеонаблюдение, у охранников при себе нет табельного оружия, а в случае ЧС используются силы группы быстрого реагирования, ценные объекты застрахованы.

2.5 Разработка системы контроля и управления доступом

Разработка СКУД на предприятии начинается с грамотной оценки всех параметров:

- Требования, предъявляемые к системе безопасности;
- Особенности помещения – масштабы предприятия, поток посетителей, количество штатных сотрудников, наличие пожарных выходов и другие детали;
- Уровень секретности отдельно взятых помещений – ограниченный допуск может потребоваться на склад с ценным товаром, в кабинет руководителя или в серверную;
- Наличие охраны – повлияет на комплект оборудования системы контроля и управления доступом на предприятии и количество зон контроля.

Для рекламного агентства «DELTAPLAN» была выбрана Профессиональная система контроля и управления доступом ParsecNET. Она использована как СКУД и система безопасности.

Офис размещен на одном из этажей бизнес-центра, и занимает правое крыло. В данном крыле 13 отдельных кабинетов, 8 из которых будут оборудованы СКУД.

Задачи:

1. Учет рабочего времени сотрудников;

2. Фото-фиксация входящих в отдельные кабинеты с использованием IP-камер;

3. Получение отчетов о перемещении и местонахождении в течение рабочего дня сотрудников;

4. Исключение возможности клонирования карт доступа.

Особенности объекта

- Двухсторонних точек прохода – 4 шт.;
- Работа офиса по расписанию (9:00 – 18:00, суббота и воскресение - выходные);
- Независимая работа от СКУД бизнес-центра.

Типовые решения:

- Система будет реализоваться на базе программного обеспечения ParsecNET Office.
- 8 рабочих кабинетов будут оборудоваться СКУД. Каждая точка прохода управляется контроллерами NC-8000. В качестве считывателей будет использоваться PNR-P19, работающие с картами Mifare Classic 1K и 4K (с поддержкой защищенного режима).
- Для фотофиксации входящих в отдельные кабинеты устанавливаются IP-камеры, которые делают снимки по событиям с сохранением данных в базу.
- Система включает сервер, к которому подключается оборудование, а также рабочая станция оператора:

Состав системы:

- Сервер, к которому подключается оборудование.

- Рабочее место администратора системы (оборудовано на сервере системы).
- Рабочая станция бухгалтерии с функциями ведения учета рабочего времени и управления персоналом.
- Рабочая станция руководителя с возможностью анализа трудовой дисциплины.
- Рабочая станция секретаря с возможностью программирования и занесения карт в БД.

Перечень оборудования:

ПО:

- PNOffice-08 – версия программного обеспечения, поддерживающая работу до 8 точек прохода;
- PNOffice-AR - Модуль учета рабочего времени с генератором отчетов; PNOffice-WS – Дополнительная рабочая станция (2 шт.).
- PNSoft-VI - Модуль интеграции с системами видеонаблюдения

Оборудование:

- Контроллер – NC-8000 (8 шт.);
- Контроллер – NC-1000 – IP (4 шт);
- Электромагнитный замок (дверь) – (8 шт.);
- Считыватели – PNR-P19 (8 шт.);
- Считыватели (для программирования и занесения карт в БД) – PR-P08 (1 шт.);
- Смарт-карта Mifare – (80шт.).

В системе ParsecNET Office будут использоваться контроллеры доступа, работающие по протоколу Ethernet.

При использовании IP-контроллеров конечная структура системы контроля и управления доступом определяется топологией локальной сети организации.

Преимущества:

Быстрая скорость передачи данных.

Недостатки:

Небольшая протяженность линии (до 100 м).

Рисунок. 2.5.1 Топология СКУД

Система контроля и управления доступом на предприятие автоматически выполняет работу сразу нескольких отделов.

Объекты, подлежащие оснащению системой контроля и управления доступа:

1. Бухгалтерия;
2. Информационно вычислительный отдел;
3. Серверная;
4. Кабинет Директора;
5. Кабинет Зам. Директора;
6. Пост Охраны;
7. Отдел творческих разработок;
8. Отдел по работе с клиентами.

Сотрудники предприятия проходят пост охраны, поднося постоянный пропуск к считывателю карт на турникете. Факт идентификации личности записывается (регистрируется время идентификации и Ф.И.О. сотрудника).

1. Бухгалтерия:

Количество пользователей: 4 постоянных.

Рубеж исполнен в виде стальной двери с двумя замками. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается

ключом. Ключ имеется у бухгалтера, главного бухгалтера, руководителя предприятия. Доступ в бухгалтерию имеют только бухгалтера, главный бухгалтер и руководитель предприятия. Их постоянный пропуск запрограммирован соответственным образом, чтобы они могли получить доступ к кабинету бухгалтерии.

2. ИВО:

Количество пользователей: 7 постоянных.

Рубеж исполнен в виде стальной двери с двумя замками. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у семи работников этого отдела.

3. Серверная:

Количество пользователей: 4 постоянных.

Рубеж исполнен в виде стальной двери с двумя замками. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у начальника отдела безопасности, главного администратора, руководителя предприятия. Доступ в серверную имеет начальник ИВО, инженеры – электронщики и руководитель предприятия.

4. Кабинет директора

Рубеж исполнен в виде обычной офисной двери. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у начальника.

5. Кабинет Зам. Директора

Рубеж исполнен в виде обычной офисной двери. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у зам. начальника.

6. Пост охраны:

Количество пользователей: 60 постоянных и посетители.

Исполнено в виде турникета, со считывателем карт. Протоколируется пропуск посетителей через проходную. Присутствует система видеонаблюдения. Турникет и считыватель карт подключены через шлейф к сетевому контроллеру доступа устройства.

7. Отдел творческих разработок

Рубеж исполнен в виде обычной офисной двери. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у работников этого отдела.

8. Отдел по работе с клиентами

Рубеж исполнен в виде обычной офисной двери. Первый замок открывается соответствующей картой доступа. Второй замок механический, открывается ключом. Ключ имеется у работников этого отдела.

2.6 Разработка подсистемы видеонаблюдения

Профессиональная система контроля и управления доступом ParsecNET будет использована интеграция с видеоподсистемой программного комплекса «Интеллект» ITV. Совместное использование СКУД с системой видеонаблюдения позволяет настроить их взаимодействие и получать информацию из нескольких источников для комплексного анализа различных ситуаций. Один из примеров такого взаимодействия — включение записи с видеокамеры по событию предоставления доступа, что позволяет фиксировать на видео людей и автотранспорт, прошедших через точку прохода.

Другой пример взаимодействия — удаленная фотоидентификация. При считывании карты доступа на экран монитора выводится фотография владельца карты из базы данных и видео с камеры, установленной на проходной. Сравнивая их, сотрудник охраны принимает решение о предоставлении доступа.

Интеграция видеоподсистемы платформы «Интеллект» в СКУД ParsecNET позволяет реализовать в системе следующий функционал: просмотр «живого» видео с камер системы видеонаблюдения (без возможности самостоятельно создавать «раскладки» камер в окне видеонаблюдения).

- привязка камеры к точке прохода или охранной области;
- просмотр связанных с событиями от точек прохода и охранных областей видеозаписей;
- ручное управление записью через монитор событий системы;
- управление записью с камер видеонаблюдения по событиям системы;

- управление записью с камер видеонаблюдения с использованием менеджера заданий;
- ретроспективный анализ событий с просмотром не только данных о событии, но и связанных с событиями видеозаписей;
- распознавание автомобильных номеров;
- включение и выключение режима охраны в видеоподсистеме (детектор движения или активности).

Мощная, функциональная подсистема видеонаблюдения платформы «Интеллект» обладает всеми преимуществами распределенной архитектуры:

- неограниченное количество видеосерверов и камер видеонаблюдения;
- удаленный мониторинг и администрирование;
- возможность установки любого количества рабочих мест, как локальных, так и удаленных.

Подсистема видеонаблюдения в составе комплекса «Интеллект» имеет мощные сетевые возможности:

- видеоархивы любых видеосерверов могут переноситься в режиме реального времени или по расписанию на выделенные серверы-архиваторы для долговременного хранения;
- каждый клиент может иметь доступ как к архиву видеосервера, так и к архивам выделенных серверов-архиваторов;
- видеопотоки могут распределяться в системе с помощью модуля «Видеошлюз», т. е. каждый следующий клиент, получающий видеопоток от конкретного сервера, не будет увеличивать нагрузку на канал связи с этим сервером;
- клиент может получить видеопоток от сервера, находящегося в другом сегменте сети, посредством «Видеошлюза».

Видеоподсистема «Интеллекта» будет использовать стандарт распространенного алгоритма видеокомпрессии — MJPEG, MPEG-4 и H.264.

На предприятии будет присутствовать комбинированная система видеонаблюдения. Внутри помещения применяются цветные камеры, для уличного наблюдения применяются черно-белые камеры, с встроенным инфракрасным прожектором.

Видеонаблюдение ведется с 4 камер внутри помещения, и с 3 уличных камер. Пост наблюдения оборудован видеорегистратором, который соединен с интегрированной системой безопасности при помощи специального интерфейса и соответствующего программного обеспечения.

Центральный сервер ProLiant DL380p Gen8 монтируется в шкафу. В этом же шкафу устанавливается 18-портовый коммутатор TSn -16P18. Для обеспечения бесперебойной работы и безаварийного функционирования системы, в шкафу устанавливается источник бесперебойного питания UPS-CP-2KVA/240AC.

ЭКОНОМИЧЕСКИЙ РАСЧЕТ

					РТК.О. 09.02.02 02 КС-16/9 ПЗ			
Изм.	Лист	№ докум	Подпись	Дата				
Выполнил		Чащина А.А.			ЭКОНОМИЧЕСКИЙ РАСЧЕТ	Литера.	Лист	Листов
Руководит.						У	29	5
Рецензент		Володькин Е.В				ГАПОУ РС(Я) «МРТК»		
Н. контр.								
Утвержд		Мусорина А.А						

3 ЭКОНОМИЧЕСКИЙ РАСЧЕТ

Заключительным этапом проектирования локальной сети является проведение стоимостной оценки компонентов сети.

Таблица 3.1 - Расчет стоимости программных средств

Название	Стоимость	Всего
Kerio Control Subscription for 3 year , 50-249 users	5 850.23 руб.	5 850 руб.
ESET NOD32 Антивирус - универсальная электронная лицензия на 1 год на 3 ПК или продление на 20 месяцев	1 490 руб.	32 780 руб.
ПО системы управления доступом Indeed Enterprise Authetication	120 030 руб.	120 030 руб.
		Итог: 158 660 руб.

Таблица 3.2 - Расчет затрат на установку видеонаблюдения

Название	Модель	Характеристика	Стоимость	Кол-во	Всего
Камера наружного видеонаблюдения Zodikam	3242-PM	Процессор Hisilicon -HI3516C; Работа с видеорегистратором; Встроенный микрофон; Съемка при слабом освещении; CDS датчик	3 780 руб.	3	11 340 руб.
Камера внутреннего видеонаблюдения VISTA VG	N332VF	Цветность изображения дисплея Цветная; Форматы файлов видео H.264, MPEG; Тип матрицы CMOS Exmor; Общее количество пикселей 2.4 Мпикс	2 970 руб.	4	11 880 руб.
Центральный сервер Hewlett-Packard	ProLiant DL380p Gen8	Процессор: Intel Xeon E5-2600 v3, от 4 до 8 ядер; Количество процессоров: 1-2; Память: RDIMM, HP DDR4, 8 слотов; Дисковая система: 4 штуки 3,5” дисков SAS/SATA.	49 900 руб..	1	49 900 руб.

Продолжение таблицы 3.2

Коммутатор TANTOS	TSn-16P18	возможность установки в стойку; 16 портов Ethernet 10/100 Мбит/сек; 2 uplink/стек/SFP (до 10/100/1000 Мбит/сек); 440 x 44 x 350 мм, 3.7 кг	20 664 руб.	1	20 664 руб.
Монитор Samsung	SMT-2233	Монитор видеонаблюдения LED; 21,5"; Разрешение: 1920x1080; Соотношение сторон: 16:9; Время отклика: 5 мс; Яркость: 250 кд/м2; Контраст: 1000:1; Видеовходы: 1xVGA, 2xBNC, 1xHDMI, 2xAudio; Видеовыходы: 1xBNC; AC 220B; OSD, PAL/NTSC; Габаритные размеры, мм 515x59.9x316	41 496 руб.	2	82 992 руб.
Видеорегистратор для систем видеонаблюдения Uniview	NVR304-32E-B	Питание DC12; Максимальная частота кадров25 к/с; Другие интерфейсы RS-485, HDMI, USB x2; Количество пользователей 128; Сетевые протоколы ONVIF, RTSP; Количество каналов записи 32; Кодеки и форматы видео H.264+, H.265+, H.264, H.265; Количество отсеков для (HDD/SSD) 4; Интерфейс подключения накопителя SATA; Максимальный объем одного накопителя 8000 Гб; Сеть Ethernet есть	19 382 руб.	1	19 382 руб.
ПО «Интеллект» ITV	-	многофункциональная открытая программная платформа, предназначенная для создания комплексов безопасности любого масштаба.	-	-	98 120 руб.
					Итог: 294 278руб.

Таблица 3.3 - Расчет стоимости компонентов системы СКУД

Наименование, модель	Характеристика	Стоимость	Кол-во	Всего
ИБП UPS-CP-2KVA/240AC	Однофазное устройство бесперебойного питания с двойным преобразованием, согласно трехступенчатому классификационному коду VFI-SS-111. Напольное устройство, по желанию монтаж на стойку 19“, поворачиваемая на 90° контрольная ЖК-панель, гнездо для платы SNMP.	153 121 руб.	1	153 121 руб.
Контроллер NC-8000-D	Сетевой контроллер на одну точку прохода, подключение по сети Ethernet, RS-485, 8 000 ключей, 16 000 событий, до 2-х считывателей, одно/двухсторонний проход, подсчет количества человек в помещении, выдача ключей с ограничением по сроку действия и количеству проходов, аварийная разблокировка, крепление на DIN-рейку, 0...+55 °C, 145x110x40 мм	14 308 руб.	8	114 464 руб.
Интерфейс NI-A01	предназначен для использования в системе контроля доступа ParsecNET. Интерфейсы служат для подключения контроллеров к USB-порту ПК.	5 684 руб.	1	5 684 руб.
Бесконтактные смарт-карты Mifare ID	Количество чипов 1; Производитель чипа NXP; Минимальная партия 200; Рабочая частота 13.56 МГц (HF); Толщина 0,76 мм; Габариты 86x54x0.8 мм; Цвет Белый; Количество штук в упаковке 100; Гарантия 1 год; Страна производства Россия	66 руб.	80	5 280 руб.

Продолжение таблицы 3.3

Турникет трипод Ростов-Дон Т9М1-02 из окрашенной стали (без планок)	Напряжение питания 12 В; Потребляемый ток, макс. 1.5 А; Габариты 745x780x995 мм; Габариты без штанг 180x404x995 мм; Ширина перекрываемого прохода 745 мм; Вес 32 кг; Рабочая температура от +1°C до +40°C; Стыковка со СКУД Любые типы СКУД	31 630 руб.	4	126 520 руб.
Считыватель PR-P18	Тип считывателя; Для компьютера; Вид считывателя Бесконтактный RFID; Исполнение Для помещений; Материал корпуса Пластик; Количество поддерживаемых форматов Одноформатный; Поддерживаемые форматы Mifare Classic, Mifare Plus, Mifare UltraLight, Mifare ID; Тип монтажа Настольный	14 602 руб.	1	14 602 руб.
Считыватель PNR-P19	Вид считывателя Бесконтактный RFID; Исполнение Для помещений; Материал корпуса Пластик; Количество поддерживаемых форматов Мультиформатный Поддерживаемые форматы Мультиформатный, Mifare Classic, Mifare ID, Mifare Plus, NFC	12 250 руб.	8	98 000 руб.
ПО «ParsescNET Parsec PNSoft-08	стандартная версия программного обеспечения с возможностью поддержки 8 точек прохода. Позволяет решать задачи управления доступом на любых типах объектов за счет гибкого изменения конфигурации системы благодаря наличию различных дополнительных программных модулей.	-	-	14 210 руб.

Продолжение таблицы 3.3

PNOffice-AR	Модуль PNOffice-AR позволяет вести полный учет и анализ рабочего времени, задавать различные критерии поиска - опоздавших, переработавших, с возможностью деления по подразделениям за любой промежуток времени.	-	-	14 700 руб.
PNSoft-VI	Модуль интеграции с подсистемами видеонаблюдения PNSoft-VI позволяет использовать информацию с видеокамер непосредственно в приложениях ParsecNET (монитор событий, модуль видеоверификации).	-	-	19 600 руб.
ALFA Электромагнитный замок HM280	Электромагнитный замок HM280 предназначен для установки на все виды входных дверей. Подходит для деревянных, пластиковых, металлических и стеклянных дверей. Применятся при монтаже СКУД, и домофонии. Модель выполнена из алюминиевого сплава, не подвержена коррозии и невосприимчива к перепадам температур и намагничиванию. Дополнительно к замку можно приобрести крепеж для различных видов монтажа и для всех видов дверей.	1 890 руб.	8	15 120 руб.
				Итог: 581 145 руб.

Суммарные затраты на разработку системы безопасности предприятия составляют 1 034 083 рубля.

ЗАКЛЮЧЕНИЕ

ЗАКЛЮЧЕНИЕ

В результате проведенной работы была разработана комплексная система защиты информации в рекламном агентстве «DELTAPLAN» которая регулярно обеспечивает защиту.

Для защиты атак из сети Интернет таких как: вирусы, черви, троянские и шпионские программы, которые засоряют сеть — выбран межсетевой Kerio Control. Он проводит глубокий анализ сетевых пакетов, обладает расширенными возможностям для маршрутизации в сети, поддерживает IPv4 и IPv6. Тонкая настройка позволяет управлять входящим и исходящим трафиком, разрешать соединения только с заданными URL, приложениями, типом трафика, категориями данных и в указанное время суток.

Для защиты пользователей от похищения личных данных на сайтах, а также сканер средств социального общения для сохранения безопасности за счет контроля над отображаемой посетителям информацией используется ESET NOD32 Antivirus. В нем антивирусный и антишпионский модуль, а также предлагает облачную поддержку для ускорения сканирования за счет проверки файлов на основе их репутации.

Резервное копирование используется для создания копий файлов и папок на дополнительные носители информации. Бэкап делается для восстановления данных, в случае если информация повредилась или разрушилась в основном месте хранения.

Программное обеспечение Indeed Enterprise Authentication – обеспечивает конфиденциальность и целостность объектов и их доступность путем запрещения обслуживания неавторизованных пользователей.

Главная задача системы контроля доступа - обеспечения надежной защиты.

Защита от проникновения на территорию лиц без права доступа - благодаря установке СКУД, на предприятие попадают только сотрудники или людей, получившие пропуск. Это средство позволит снизить риск краж и повреждений оборудования, обеспечить безопасность деятельности работников. Контроль за прохождением персонала на территорию объекта, а также сбор информации о длительности пребывания. Это средство необходимо для точного расчета отработанного времени, которое учитывается при сдельной оплате труда.

Перечисленные функции системы осуществляются при помощи программных режимов. Основной режим предполагает проход в зону охраны СКУД по индивидуальным картам-пропускам. Программное обеспечение системы позволяет установить:

- защиту от повторного прохода. СКУД запрещает вновь использовать пропуск, если не был совершен выход из охраняемой зоны. Запрет повторного прохода помогает избегать несанкционированного доступа, подделки пропусков. Такая функция также позволит задать определенную очередность прохождения зон, запретив другие маршруты.
- доступ для нескольких лиц. СКУД открывает проход, только если считывает заданное число идентификаторов соответствующего уровня доступа. Режим позволяет надежно защитить зоны повышенной секретности.
- контроль блокировки двери. Через программу устанавливается определенное время, в которое дверь находиться в открытом положении. Если система фиксирует нарушение этого срока, передается сигнал охраннику. Это средство помогает выявить случаи незаконного прохождения на территорию нескольких людей по одному пропуску.

Обеспечения защиты и сбора информации выполняться эффективно, когда СКУД подключен к системе видеонаблюдения. Качественное программное обеспечение также дает возможность расшить средства контроля.

Усиленная аутентификации реализуемая продуктом Indeed Enterprise Authentication интегрируется с системой СКУД от ParsecNET Office, которая в свою очередь взаимодействует с системой видеонаблюдения, это дает возможность круглосуточного наблюдения и высокой защиты информации.

Если в рекламном агентстве «DELTAPLAN» принять меры, описанные в данной работе, предприятия будет иметь большую гарантию защиты от потери данных.

Но никакие средства защиты не могут гарантировать стопроцентную безопасность данных сети.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

					РТК.О. 09.02.02 02 КС-16/9 ПЗ			
Изм.	Лист	№ докум	Подпись	Дата				
Выполнил		Чащина А.А.			СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	Литера.	Лист	Листов
Руководит.						у	37	2
Рецензент		Володькин Е.В				ГАПОУ РС(Я) «МРТК»		
Н. контр.								
Утвержд		Мусорина А.А						

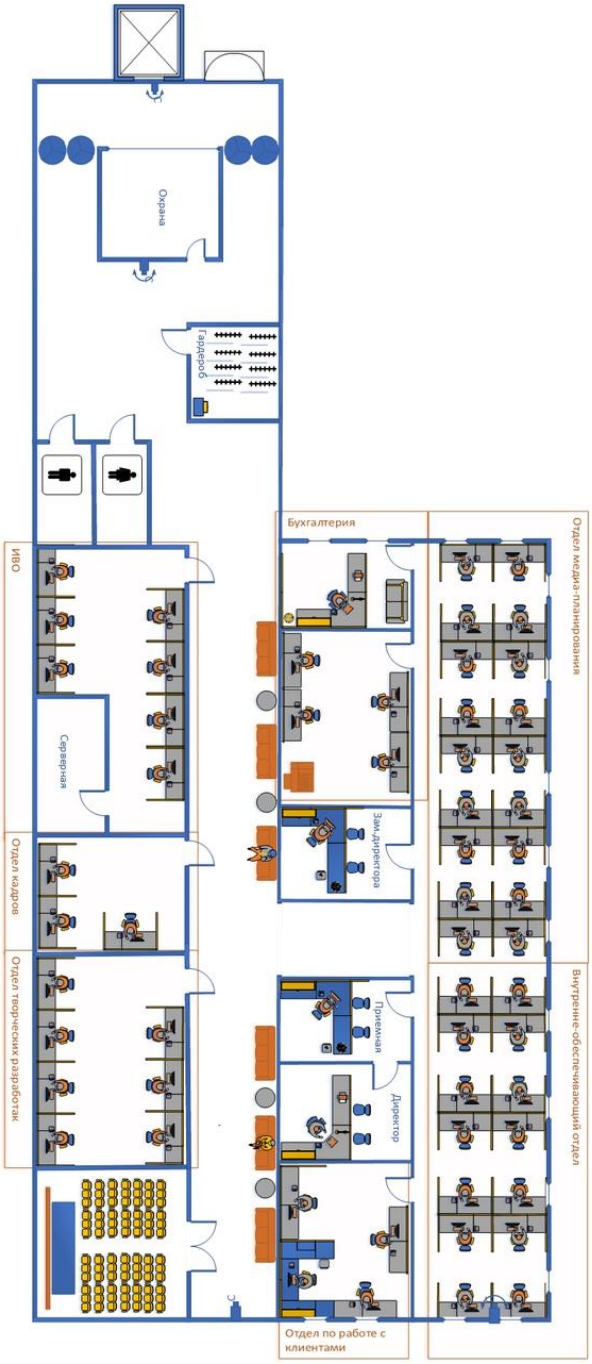
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб: Питер, 2008.
2. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008.
3. Доля А.В. Внутренние угрозы ИБ в телекоммуникациях. 2007.
4. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ.
5. Биячуев, Т.А. Безопасность корпоративных сетей. – СПб: ГУ ИТМО, 2004.
6. С.Вихорев, Р.Кобцев Как определить источники угроз. – Открытые системы. 2002.
7. Федеральный закон «Об информации, информатизации и защите информации».
8. Президент Российской Федерации. Указ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
9. Л.Хофман, «Современные методы защиты информации», - Москва, 2005.
10. П.Зегжда, «Теория и практика. Обеспечение информационной безопасности». - Москва, 2006.
11. Гостехкомиссия России. «Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения», - Москва, 1992.
12. Журналы "Защита информации" №№ 1-8 изд. КОНФИДЕНТ, С-Пб.

ПРИЛОЖЕНИЕ А

ПРИЛОЖЕНИЕ А

План здания



ПРИЛОЖЕНИЕ Б

ПРИЛОЖЕНИЕ Б

Схема подключений устройств на предприятии