Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Разработка информационно-аналитической системы конфиденциального делопроизводства на базе ИСУБД "Cronos"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 520
_____ Мамай, С. В.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 9
1. СОДЕРЖАНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В КОНФИДЕНЦИАЛЬНОМ ДОКУМЕНТООБОРОТЕ 12
1.1. Общие понятия и определения информационно – аналитической деятельности 12
1.2. Сущность и значимость информационно – аналитической деятельности в конфиденциальном документообороте 18
1.3. Сравнительный анализ существующего программного обеспечения для создания информационно – аналитической системы конфиденциального делопроизводства 20
1.4. Вывод по первой главе 23
2. ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА 24
2.1. Понятие, цель и принципы организации конфиденциального документооборота 24
2.2. Правила организации конфиденциального документооборота 26
2.3. Угрозы и риски конфиденциального документооборота 27
2.4. Документирование конфиденциальных сведений 29
2.5. Гриф конфиденциальности документа 30
2.6. Носители конфиденциальной информации 31
2.7. Санкционирование изготовления и составление текста конфиденциального документа 33
2.8. Учет и изготовление конфиденциального документа 34
2.9. Издание конфиденциального документа 36
2.10. Вывод по второй главе 37
3. ПРЕДВАРИТЕЛЬНОЕ ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ СИСТЕМЫ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА 38
3.1. Основные понятия ИСУБД CronosPro 38
3.1.1. Базы данных, записи, поля и значения 39
3.1.2. Запись базы данных 39
3.1.3. Поле записи 40
3.1.4. Свойства полей 40
3.1.5. Словарный банк данных 41
3.1.6. Использование запросов для поиска данных 42

3.2. Постановка задачи 42
3.3. Описание предметной области 43
3.4. Определение баз данных и их полей 44
3.5. Определение связей между базами данных 52
3.6. Создание форм для работы пользователя 54
3.7. Вывод по третьей главе 57
4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 58
Введение 58
4.1. Рекомендации по организации рабочего места пользователя 58
4.1.1. Требования к помещениям для размещения рабочего места 58
4.1.2. Требования к уровням шума на рабочих местах 59
4.1.3. Требования к освещению на рабочих местах 60
4.1.4. Общие требования к организации рабочих мест пользователей 61
4.1.5. Требования к электробезопасности 63
4.1.6. Рекомендации по организации режима труда и отдыха пользователя 64
4.2. Пожарная безопасность 66
4.3. Микроклимат 74
4.4. Вывод по четвертой главе 75
ЗАКЛЮЧЕНИЕ 76
ПРИЛОЖЕНИЕ А 77
ПРИЛОЖЕНИЕ Б 121
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 122

ВВЕДЕНИЕ

Базовым понятием всех информационных технологий является информация. Любая деятельность человека представляет собой процесс сбора и переработки информации, принятия на ее основе решений и их выполнения. С появлением современных средств вычислительной техники информация стала выступать в качестве одного из важнейших ресурсов научно-технического прогресса.

Согласно ст. 2 Федерального закона РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация это сведения (сообщения, данные) независимо от формы их представления.

В соответствии со ст. 5 вышеуказанного закона, в зависимости от категории доступа к информации она делится на общедоступную и информацию ограниченного доступа. В свою очередь к информации ограниченного доступа относится государственная тайна и конфиденциальная информация. Исходя из Указа Президента от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера», к видам конфиденциальной информации, можно отнести:

1. Персональные данные;
2. Коммерческую тайну;
3. Служебную тайну;
4. Профессиональную тайну;
5. Тайну следствия и судопроизводства;
6. Сведения о сущности изобретения.

В целях регулирования отношений, касательно информации, которая несет в себе действительную или потенциальную коммерческую ценность по причине неизвестности ее третьим лицам, 29 июля 2004 года был издан Федеральный закон “О коммерческой тайне”.

Основой информационных потоков любого предприятия, организации или учреждения составляют различные документы, создаваемые для фиксаций распоряжений, указов и различных фактов.

На основании вышеизложенного, все документы на предприятии, в организации или учреждении можно разделить на две основные группы:

1. Информацию открытого доступа;
2. Информацию ограниченного доступа.

Движение этих документов или документооборот также можно разделить на открытый или конфиденциальный.

Применительно к коммерческому предприятию, согласно Федеральному закону от 29.07.2004 N 98-ФЗ “О коммерческой тайне”, создание конфиденциального документооборота является обязательным условием формирования режима коммерческой тайны.

Система конфиденциального документа оборота достаточна сложна, ведь современные организации представляют собой структуру из различных подразделений и сотрудников этих подразделений. У каждого сотрудница есть свои обязанности и уровень допуска информации с которой он может работать. В связи с этим усложняется задача защиты конфиденциальной информации и разработка системы конфиденциального документооборота должна учитывать все вышеперечисленные аспекты.

Для обеспечения функционирования и более эффективного контроля документооборота требуется информационно – аналитическая система. Сложность создания такой системы заключается не только в правильной постановке задачи, но и в верном выборе инструмента создания.

Таким образом, актуальность данной работы заключается в разработке информационно – аналитической системы конфиденциального делопроизводства, прежде всего на коммерческом предприятии.

Предметом выпускной квалификационной работы является информационно-аналитическая система конфиденциального производства на базе ИСУБД “Cronos”.

Целью ВКР является создание информационно – аналитической системы конфиденциального делопроизводства, для документов составляющих коммерческую тайну.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Обеспечить создание режима коммерческой тайны на предприятии;
2. Обеспечить контроль конфиденциального документооборота на предприятии.

1. СОДЕРЖАНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В КОНФИДЕНЦИАЛЬНОМ ДОКУМЕНТООБОРОТЕ

1.1. Общие понятия и определения информационно – аналитической деятельности

Основополагающим принципом системного подхода в изучении, является принцип диалектики Сократа, согласно которому прежде чем приступить к обсуждению какого – либо вопроса, необходимо определиться в соответствующих понятиях, чтобы не получился разговор в одних и тех же терминах, но о разном. Поэтому необходимо зафиксировать определения этих понятий.

Информационно – аналитическая деятельность предполагает получение нового знания (или информации) в процессе исследования. Поэтому для начала определимся с соотношением понятий «данные» и «информация» и ответим на вопрос: любые ли данные можно считать информацией?

Федеральный закон №149 – ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации» определяет информацию как сведения (сообщения, данные) независимо от формы их представления [1].

Информация имеет следующий ряд определений:

1. Американский инженер, криптоаналитик и математик, «Отец информационного века» К. Шеннон определил информацию как сообщение, уменьшающее неопределенность [2]. В данном случае информативность можно трактовать как степень снятия им неопределенности;

2. Американский учёный, выдающийся математик и философ, основоположник кибернетики и теории искусственного интеллекта Н. Винер определили информацию как обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств [3];

3. В словаре американского национального стандарта по информационным технологиям (American National Standard Dictionary of Information Technology

ANSDIT) данные определяются как некоторое представление, которому может быть приписан некоторый смысл на основе общепринятого в обществе или специального соглашения (кодирования). Мерой возможной информативности данных является их разнообразие [4];

4. Исследователь «аномальных явлений» Ю.А. Фомин, а в последствии и доктор информациологических, физико-математических и технических наук, профессор Московского технологического института бытового обслуживания И.И. Юзвишин определили информацию как неотъемлемое свойство материи, как форму ее существования [5, 6];

5. В словаре американского национального стандарта по информационным технологиям (American National Standard Dictionary of Information Technology ANSDIT) информация определяется как смысл, присваиваемый данным их получателем посредством применения специального соглашения (кодирования) [4];

Известно, что назначение понятия – это выделение и обобщение предметов под одним названием (термином) по их отличительным признакам. При этом понятие имеет большую научную значимость, чем более строго оно выделяет определяемые предметы и использует существенные отличительные признаки [7].

Исходя из этого менее подходящим, можно считать определение Фомина – Юзвишина, так как оно не полно как в отношении выделения, так и в отношении признаков. Кроме этого, нет никаких научных оснований утверждать, что информация – неотъемлемое свойство материи и форма ее существования.

Определение из Федерального закона РФ не раскрывает понятие «сведения», но при этом сведения и информацию представляет как синонимы.

По нашему мнению, наиболее подходящим определением понятия «информация» можно считать определение ANSDIT, так как оно четко разграничивает понятия «данные» и «информация». Использует наиболее существенные признаки информации – данные, их получателя, соглашение, определяющее способ выявления смысла данных, смысл данных.

Для того чтобы преобразовать данные в информацию нужно:

1. Выделить смысл данных, интерпретируя их в системе знаний получателя;

2. Этот смысл поместить в контекст, который снимет какую – то неопределенность.

Сложный процесс исследования, предполагает получение нового знания (информации), что является технологией информационно – аналитической деятельности. На сегодняшний день существует множество определений понятия «информационно – аналитическая деятельность».

Конопатов С.Н. и Пинигин В.В. в своей статье определили информационно – аналитическую деятельность как организованный целенаправленный процесс информационно – познавательного обеспечения управления. Включающий информационно – справочную работу, информационно – аналитическую работу и информационное взаимодействие [8].

Такие специалисты как Кулицкий С.П. [9], Кузнецов И.М. [12], Степанов Е.А. и Корнеев И.К. [11], Конотопов П.Ю., Курсонов Ю.В. [10] в своих работах рассматривают информационно – аналитическую деятельность как процесс в сфере управления, представляющий собой процесс поиска, сбора, переработки и представления информации в форме, пригодной для ее использования; как информационно – аналитическую работу в двух аспектах – информационную работу и аналитическую работу; как системное получение, анализ и накопление информации с элементами прогнозирования с вопросов, касающихся деятельности учреждения [13].

Опираясь на различные подходы к определению понятия «информационно – аналитическая деятельность» Захаров И.В. и Филипов Л.Я. сформулировали обобщенное определение понятия «информационно – аналитическая деятельность» под которой в дальнейшем мы будем понимать: «совокупность информационных процессов (сбор, поиск, переработка информации), необходимых для качественного и эффективного процесса контроля» [13].

Исходя из этих определений мы в своей работе будем рассматривать информационно – аналитическую деятельность направленную на сферу контроля и придерживаться ее разделения на информационную и аналитическую работу.

Так по его мнению к средствам информационной работы можно отнести «совокупность документальных, технических и других устройств, предназначенных для накопления, обработки, систематизации, хранения и выдачи информации» [12, С. 17], а к средствам аналитической работы Кузнецов И.М. относит законы и методы мыслительной деятельности, а также другие технические средства, на основе и с помощью которых осуществляется обработка фактических данных с более высоким качеством [12]. Поэтому технология аналитической работы предполагает получение нового знания (выводной информации), которое обеспечивает сложный процесс исследования.

Одной из составляющих информационно – аналитической деятельности, является понятие «информационно – аналитическая работа», которая также как и информационно – аналитическая деятельность делиться на два уровня:

1. Информационный уровень – заключающаяся в поиске, сборе, хранении, распространении информации;
2. Аналитический уровень – заключающийся в обобщении, классификации информации, ее анализе и преобразовании, разработке выводов, предложений, рекомендаций и прогнозов [6].

С позиций принятия решений различают оперативный, тактический, стратегический уровни информационно – аналитической работы.

Основными формами информационно – аналитической работы являются:

1. Мониторинг, включающий информационные сводки и обзоры;
2. Анализ эффективности принятия решений;
3. Исследование актуальных проблем (информационные разработки, оперативные исследования, аналитические исследования [6].

Основываясь на выделенных формах информационно – аналитической работы можно выделить следующие методологические аспекты информационно – аналитической работы:

1. Формирование цели исследований;
2. Создание понятийного аппарата;
3. Обеспечение достаточной информированности;
4. Раскрытие значения фактов;
5. Установление причин и следствий;
6. Определение тенденций развития;
7. Обеспечение высокого уровня достоверности;
8. Формирование выводов и рекомендаций;
9. Наличие обратной связи [6].

Основополагающее значение в организации аналитической работы имеют следующие принципы:

1. Целеустремленность – ориентация аналитической деятельности на достижение конкретных целей для решения определенных задач, как результатов практической деятельности;
2. Актуальность – аналитическая деятельность должна отвечать потребностям практики, иметь высокую степень важности на данный момент, в данной ситуации, для решения конкретной проблемы;
3. Активность – проведение информационно – аналитической деятельности и выдача ее результатов с элементами прогнозирования;
4. Достоверность – учет достоверности исходных данных анализа, точности количественных данных, используемых степени объективности и обоснованности выводов, оценок, предложений;
5. Полнота – использование всей имеющейся информации, имеющей отношение к решению поставленных задач;
6. Обоснованность – получение аргументированных результатов аналитической работ;

7. Своевременность – получение и выдача результатов информационно – аналитической деятельности в нужные сроки, в удобной форме и виде, что пригодна для пользования;

8. Непрерывность – организация постоянно действующего информационно – аналитического мониторинга обстоятельств, своевременное отражение основных изменений;

9. Гибкость – возможность быстрой адаптации системы к изменениям без модификации структуры методов и средств реализации аналитической работы [6].

Методология аналитических исследований – это совокупность принципов, методов, способов и подходов к организации и проведению исследований: принципы – выработанные наукой и практикой, сформулированы в концентрированном виде наиболее важные идей, установки, метод – совокупность приемов и способов познания, прием – отдельное действие для достижения цели исследования, способ – система действий, применяемых при исполнении определенного исследования; процедура – установленный порядок выполнения приемов и способов исследования, методика – последовательность конкретных процедур, реализация которых обеспечивает достижение цели исследований, технология (техника) аналитических исследований – совокупность приемов и способов, которые входят в состав процедуры [6].

Для достижения определенных целей аналитических исследований используют средства информационно – аналитической работы – это совокупность интеллектуальных и технических средств, обеспечивающих выполнение поставленных целей [6].

Интеллектуальные средства информационно – аналитической работы включают: сведения – характеристики свойств объекта наблюдается или исследуется, представленные в доступной форме для человека; данные – факты или сведения, представленные в формализованном виде, что обеспечивает возможность их хранения, обработки и передачи; сообщение – форма подачи информа-

ции – совокупность логически связанных сведений, представляющих для потребителя единое целое [13].

Технические средства информационно – аналитической работы включают: каталоги, дневники, информационные и информационно – аналитические системы, системы информационного обслуживания, системы искусственного интеллекта, экспертные системы, АРМ аналитиков [13].

1.2. Сущность и значимость информационно – аналитической деятельности в конфиденциальном документообороте

Руководствуясь определениями, данными в параграфе 1.1. мы рассмотрим сущность информационно – аналитической деятельности. В организации работу в области информационно – аналитической деятельности выполняют специальные информационно – аналитические подразделения. В нашем случае, работа с информационно – аналитической системой конфиденциального делопроизводства предстоит отделу канцелярии.

Цели и задачи информационно – аналитических подразделения конкретизируются применительно к уровню управления и конкретной обстановке в положениях об информационно – аналитическом подразделении организации, а также планами информационной работы и другими документами. Информационно – аналитическое подразделение реализует свое предназначение путем информационно – аналитической деятельности, включающей в себя информационно – справочную (ИСР), информационно – аналитическую работу (ИАР), информационное взаимодействие [8].

Основные задачи информационно – аналитической деятельности:

1. Информационно-познавательное обеспечение процесса управления;
2. Совершенствование информационного обеспечения управления постоянным развитием сети источников информации и совершенствованием информационной работы [8].

Опираясь на все выше сказанное мы можем сделать вывод о том, что для того чтобы произвести качественный анализ текущего состояния конфиденциального оборота в организации необходимо выполнить большую информационно - аналитическую работу. Информационно – аналитическая деятельность в конфиденциальном документообороте необходима для большего контроля и эффективности самого конфиденциального документооборота.

Из-за постоянного увеличения объема обрабатываемой информации в организации, увеличения производительности и оперативности, повышения эффективности работы, снижения прямых затрат человеческого труда необходимо автоматизировать процесс информационно – аналитической деятельности.

Для того чтобы автоматизировать данный процесс на сегодняшний день существует множество различных информационных систем, которые помогают нам:

1. Предупредить ошибки еще на этапе ввода информации;
2. Увеличить эффективность и производительность работы отдела конфиденциального делопроизводства;
3. Улучшить и облегчить использование накопленной информации;
4. Увеличить скорость доступа к информации.

Несмотря на то, что существует множество ИС для автоматизации информационно – аналитической деятельности, наша ИС для автоматизации ИАД в конфиденциальном документообороте должна удовлетворять ряду требований, а именно:

1. Оперативное удовлетворение информационных потребностей потребителя;
2. Корректный отбор первичных сведений;
3. Правильная систематизация и классификация информации;
4. Обеспечение непрерывного отбора и систематизации информации;
5. Отсутствие дублирования информации;
6. Контроль корректности информации;
7. Возможность многократного использования информации.

1.3. Сравнительный анализ существующего программного обеспечения для создания информационно – аналитической системы конфиденциального делопроизводства

В данное время для создания различного рода информационных систем используются так называемые системы управления базами данных (СУБД), которые отличаются своим функционалом и требованиями к вычислительным мощностям компьютеров клиентов СУБД так и требованиями к серверам.

В данной части главы мы будет анализировать различные серверные СУБД. При подборе базы данных важным моментом является то, что нужно выбирать базу, которая бы соответствовала в наибольшей мере предъявляемым требованиям к информационной системе, это означает что мы должны понимать какая именно модель автоматизации должна быть реализована, в нашем случае это модель конфиденциального документооборота.

При выборе СУБД сперва следует обратить внимание на следующие аспекты:

1. Требования для установки клиентского ПО;
2. Требования к аппаратным компонентам сервера;
3. Требования к серверной операционной системе.

Большую популярность сегодня имеют различные сервера на базе данных SQL. Для анализа вариантов построения информационно – аналитической системы мы подробно разберем следующие ведущие серверные СУБД:

1. Oracle;
2. IBM DB2;
3. 1С Документооборот;
4. ИСУБД «CronosPRO».

И сравним их по следующим основным аспектам:

1. Характеристика системы;
2. Настройка, обработка запросов;
3. Разработка дополнительных модулей;

4. Наличие лицензий и сертификатов;
5. Встроенные функции для анализа информации.

Для начала стоит кратко описать каждую из СУБД.

Oracle–широкое распространение Oracleполучила из-за высокого функционала, большого количества специалистов по данной СУБД. Также довольно большое русское сообщество специалистов, великое число различных технических вебинаров, в том числе и в высших учебных заведениях.

IMBDB2 –относится к семейству СУБД, производства корпорацией IMB. Особенностью является отсутствие собственных средств аутентификации, DB2 использует встроенные средства операционной системы, тем самым происходит авторизация пользователей, аутентифицированных системой.

1С Документооборот –программное обеспечение российского производителя 1С, данный продукт разработан с использованием платформы 1С:Предприятие.

CronosPro–разработка российской компании Кронос-Информ. Основным направлением при создании данного продукта был акцент на быстродействие и обеспечение информационной безопасности.

После краткого ознакомления с продуктами, стоит сравнить их по основным аспектам, перечисленным ранее. Данные представлены в таблице 1.

Таблица 1. Сравнительные характеристики СУБД

Название продукта	Минимальные требования к пк	Гибкость настройки	Возможность разработки доп. модулей	Наличие встроенных функции для анализа информации	Лицензии и сертификаты
Oracle	ОЗУ – 2Гб HDD – 3Гб ОС Windows server 2008	Зеркалирование данных, Импорт и экспорт данных	присутствует	нет	нет
IBM DB2	ОЗУ – 2Гб HDD – 1Гб ОС Windows/linux	Импорт и экспорт данных, Резервное копирование	присутствует	нет	нет
1С Документооборот	В зависимости от устанавливаемого дистрибутива	Импорт и экспорт данных, Резервное копирование И.т.д.	присутствует	конструктор отчетов	Сертификаты соотвествияФСТЭК
CronosPRO	ОЗУ – 256мб(для windows xp) HDD – 15мб ОС Windows	Импорт и экспорт данных, Резервное копирование И.т.д.	присутствует	Конструктор отчетов, построение графического отображения связей и.т.д	Сертификаты соотвествия ФСТЭК, Лицензии ФСТЭК и ФСБ

Исходя из проанализированных данных, мы видим небольшие отличия между СУБД, но самый широкий функционал остается у разработки компании Кронос-Информ под названием: CronosPro. Кроме этого, ИСУБД CronosPro может полностью удовлетворить все требования, предъявляемые к информационным системам.

Также стоит понимать, данное сравнение не является универсальным и под каждую задачу требуется отдельный анализ для выбора ПО. Наш выбор пал на ИСУБД CronosPro т.к дополнительно имеется очень широкий функционал позволяющий еще на этапе проектирования структуры баз и банка данных достаточно гибко настроить систему.

1.4. Вывод по первой главе

В первой главе были даны общие понятия и выделена значимость информационно – аналитической деятельности в конфиденциальном документообороте. Проведен анализ имеющихся продуктов на рынке и выбран инструмент для разработки информационно – аналитической системы конфиденциального делопроизводства.

2. ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА

2.1. Понятие, цель и принципы организации конфиденциального документооборота

Конфиденциальный (от латинского confidential - доверие) документ – доверительный, секретный. В ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» конфиденциальность информации определена как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

С учетом выше сказанного, мы попытались сформулировать определение конфиденциального документооборота как контролируемое движение конфиденциальной документированной информации на предприятия с момента ее первичного фиксирования на материальном носителе или получения конфиденциальных документов, отправления, передачи на архивное хранение и до момента её уничтожения или исключения ее из разряда конфиденциальной.

Целью конфиденциального документооборота является обеспечение исполнения и использования документов. В процессе движения документов нужно создавать условия для их сохранности, ибо утрата исключает возможность их исполнения и использования. Вместе с тем важной отличительной чертой и особенностью конфиденциального документооборота является необходимость защиты документов от несанкционированного доступа к ним с целью предотвращения утечки конфиденциальной информации. Вследствие этого организация конфиденциального документооборота должна строиться на основе следующих принципов:

1. Исключения несанкционированного доступа к конфиденциальным документам;

2. Целенаправленного регулирования процессов движения конфиденциальных документов;

3. Исключения инстанций прохождения конфиденциальных документов и действий с ними, не обусловленных характером и порядком исполнения документов;

4. Фиксированной передачи конфиденциальных документов;

5. Обеспечения своевременного и качественного исполнения конфиденциальных документов;

6. Персональной и обязательной ответственности за выдачу неправомерных разрешений на ознакомление с конфиденциальными документами и на их отправление.

Поскольку правила работы с конфиденциальными документами содержат в себе значительное количество правовых положений, а нарушение ее требований, приводящее, как правило, к разглашению конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую и в некоторых случаях уголовную ответственность виновных лиц, то ее следует закреплять в специальном нормативном документе, который обычно называется «Инструкция по конфиденциальному делопроизводству».

Положение должно основываться на вышеизложенных подходах и может включать в себя следующие разделы.

1. Общие положения;

2. Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации;

3. Работа с входящими, исходящими и внутренними конфиденциальными документами;

4. Группировка конфиденциальных документов в дела;

5. Хранение конфиденциальных документов;

6. Тиражирование конфиденциальных документов;

7. Уничтожение конфиденциальных документов.

Инструкция должна разрабатываться руководителем предприятия и начальниками структурных подразделений. Оно подписывается разработчиками, визирует-

ся всеми лицами, имеющими право давать разрешение на доступ к конфиденциальным документам, и утверждается приказом руководителя организации. В приказе определяются и мероприятия по введению инструкции в действие (порядок изучения инструкции пользователями, технология осуществления контроля за его выполнением и др.). С утвержденной инструкцией должны быть ознакомлены под расписку все сотрудники организации, работающие с конфиденциальными документами.

В ходе выполнении данной выпускной квалификационной работы нами было разработана данная инструкция, которую можно посмотреть в Приложении А.

2.2. Правила организации конфиденциального документооборота

Конфиденциальный документооборот имеет целью защиту документов от несанкционированного доступа, уничтожения и пресечения утечки конфиденциальной информации. Конфиденциальный документооборот – это защищенный документооборот, а защищенный документооборот – это движение конфиденциальных документов по пунктам обработки в жестких условиях обеспечения безопасности носителя информации и самой информации.

Для защиты от несанкционированного доступа и распространения недостаточно мер, которые предпринимаются в рамках конфиденциального документооборота. Потому мы сформулировали наиболее важные правила конфиденциального документооборота:

1. Централизация всех процедур по хранению и обработке конфиденциальных документов;
2. Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта существования документа;
3. Учет всех конфиденциальных документов, включая копии;
4. Выполнение любых перемещений конфиденциальных документов и других операций под роспись руководителей, исполнителей и персонала;

5. Проверка целостности и комплектности, документа при любом перемещении конфиденциальных документов;

6. Фиксация всех обращений работников к документу;

7. Обеспечение и учет сохранности документов;

8. Письменное санкционирование процедур копирования конфиденциальных документов, контроль выполнения этих процедур;

9. Коллегиальность процедуры уничтожения документов и баз данных;

10. Строгий контроль выполнения работниками правил работы с такими документами, делами и базами данных.

2.3. Угрозы и риски конфиденциального документооборота

Любая деятельность всегда связана с созданием, использованием и хранением значительных объёмов информации и документов, которые представляют конкретную ценность для организации и подлежат защите от различных видов угроз.

Виды угроз конфиденциальных документов в документообороте организации можно разделить на несколько групп:

1. Несанкционированный доступ постороннего лица к документам, делам, базам данных за счет его любопытства или обманных, провоцирующих действий, а так же случайных или умышленных ошибок персонала фирмы;

2. Утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения;

3. Утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, использования остаточной информации на бумаге, дисках и различных съемных электронных носителях информации, ошибочных действий персонала;

4. Подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения;

5. Случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов;

6. Кража (хищение) документа или отдельных его частей, носителя чернового варианта документа (проекта документа) или рабочих записей;

7. Несанкционированное копирование бумажных и электронных документов, запоминание текста документа;

8. Тайное или разрешенное ознакомление сотрудника фирмы с документом и сообщение информации злоумышленнику;

9. дистанционный просмотр документов и изображений на мониторе персонального компьютера с помощью технических средств;

10. Ошибочные (умышленные или случайные) действия персонала при работе с документами (нарушение инструкции по конфиденциальному документообороту, правил обращения с документами и др.);

11. Уничтожение документов в условиях экстремальных ситуаций.

Для электронных документов угрозы особенно реальны, так как факт кражи информации практически трудно обнаружить. В отношении конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, по мнению ряда специалистов, классифицируется по степени риска следующим образом:

1. Непреднамеренные ошибки пользователей, системных администраторов и других лиц, обслуживающих информационные системы;

2. Кражи и подлоги информации;

3. Стихийные ситуации внешней среды;

4. Заражение вирусами.

2.4. Документирование конфиденциальных сведений

Процесс документирования конфиденциальной информации насыщен специфическими технологическими этапами и процедурами. Выделяются следующие основные этапы:

1. Получение разрешения руководителя своего структурного подразделения на документирование конфиденциальной информации;
2. Установления уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ;
3. Установление пункта перечня к которому относится информация;
4. Оформление и учет носителя для документирования конфиденциальной информации;
5. Составление вариантов и черновика текстов документа;
6. Получение разрешения руководителя своего структурного подразделения на изготовления документа;
7. Учет подготовленного черновика конфиденциального документа;
8. Изготовление проекта конфиденциального документа;
9. Регистрация конфиденциального документа в канцелярии.

Для решения вопроса о присвоении будущему документу грифа конфиденциальности должно быть получено разрешение руководителя структурного подразделения на составление этого документа. Как правило, для типовых категорий документов такое разрешение определяется наличием данного типа документа в утвержденном руководителем фирмы перечне ценных и конфиденциальных документов фирмы. При отсутствии предполагаемых документов в этом перечне вопрос издания решается индивидуально, решение руководителя фиксируется им на носители, предназначенном для составления черновика данного документа.

2.5. Гриф конфиденциальности документа

Своевременное установление грифа конфиденциальности сведений, подлежащих включению будущих документов, является одним из основных элементов защиты документированной информации, позволяющих обеспечить относительно надежную безопасность секретов фирмы.

Система грифования (маркирования) документов не гарантирует сохранность информации, однако позволяет четко организовать работу с документами.

Гриф конфиденциальности представляет собой реквизит (элемент, служебную отметку, помету, пометку) формуляра документа, свидетельствующий о конфиденциальности содержащихся в документе сведений и проставляемый на самом документе или сопроводительном письме к нему. Гриф ставится на всех экземплярах документа, учетных и отчетных формах, черновиках, вариантах и копиях, в которых содержаться хотя бы один из конфиденциальных показателей.

Информация и документы, отнесенные к коммерческой тайне, также имеют отметку об отнесении документа к определенному пункту перечня, соответствующих различным степеням конфиденциальности информации.

На ценных, но не конфиденциальных документах может проставляться пометка (отметка, надпись, штамп), предполагающая особое внимание к сохранности таких документов. Например: "Собственная информация фирмы", "Информация особого внимания", "Копии не снимать", "Хранить в сейфе" и др.

Изменения или снятие грифа конфиденциальности документа производится при изменении степени ценности содержащейся в нем информации. Основаниями для этих действий являются:

1. Соответствующая корректировка перечней конфиденциальных сведений или документов фирмы;
2. Истечением установленного срока действия грифа;
3. Наличия события, при котором гриф должен быть изменен или снят;
4. Установления факта неправильности присвоения грифа к документу.

Процедуры изменения и снятия грифа конфиденциальности с документов фирмы должны быть четко регламентированы.

При изменении или снятия грифа руководитель делает отметку на самом документе и в сопроводительном письме путем зачеркивания грифа или написания нового указания основания для выполнения этого действия и проставления подписи и даты. После снятия грифа документ передается в службу открытого делопроизводства фирмы.

2.6. Носители конфиденциальной информации

Следующим принципиально важным вопросом, решаемым заблаговременно руководством фирмы до начала составления текста документа, является определение необходимости предварительного учета носителя, на котором будут формироваться черновик и беловик документа. Назначение этапа учета носителя конфиденциальной информации состоит в том, что бы обеспечить безопасность информации, контроль за её сохранностью не только в подлиннике документа, но и во всех черновых материалов, вариантах и редакциях документа, отдельных записях и подготовительных материалов. На чистом носителе информации ставится избранный гриф конфиденциальности будущего документа.

Носителями документированной конфиденциальной информации могут быть:

1. Для традиционных текстовых документов - блокнот с отрывными листами и корешком, выполняющие функцию учета листов, нанесения отметок о целевом их использовании; рабочая и стенографическая тетради для больших по объему документов; отдельные пронумерованные листы бумаги, типографические формы и бланки документов;
2. Для чертежно-графических документов - пронумерованные листы ватмана, кальки, пленки, координатной бумаги и т.п.;
3. Для электронных документов - маркированные и пронумерованные, диски, флеш-накопители и т.п.;

4. Для аудио- и видеодокументов - маркированные и пронумерованные кассеты с магнитной пленкой, диски, кассеты с кинопленкой и т.п.;

5. Для фотодокументов - маркированные и пронумерованные кассеты с фотопленкой, фотобумага, микрофиши, слайды, кассеты с микрофотопленкой и т.п.;

Основными задачами учета носителей конфиденциальной информации можно назвать следующие:

1. Закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;

2. Присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки наличия;

3. Документирование фактов перемещения носителя между руководителями и сотрудниками фирмы, закреплением персональной ответственности за его сохранность.

Все типы носителя конфиденциальной документированной информации должны быть учтены до начала составления на них проекта черновика, вариантов и беловика будущего документа. Учет носителей целесообразен только на уровне руководства организации, так как именно здесь концентрируется вся действительно ценная информация.

Обязательному инвентарному учету и маркировке на всех уровнях управления и в любых структурах подлежат носители информации, для которых угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений.

Этап оформления и учета носителей конфиденциальной информации и выдачи их руководителям или сотрудникам фирмы выполняются – подразделением конфиденциального делопроизводства, решающим следующие задачи обеспечении защиты и контроля информации:

1. Предотвращение выдачи носителя лицу, несвязанному с составлением конкретного документа или исключенного из состава лиц, допускаемых данному носителю;

2. Выявление факта утраты носителя или его частей, организации поиска носителя и проведения совместно со службой безопасности фирмы служебного расследования;

3. Предотвращения нарушения принципа персональной ответственности за сохранность носителя и фиксируемой в нем информации;

4. Обнаружения фактов обмена носителя другим, фальсификации части носителя;

5. Обнаружение фактов случайной или умышленной порчи носителя, изменение формата, нумерации листов, вырывания листов и их загрязнения, склеивания и т.п.;

6. Предотвращения несанкционированной и не неоправданной деловой необходимостью передачи носителя между руководителями и сотрудниками;

7. Предотвращение несанкционированного ознакомления посторонних лиц с содержанием информации, зафиксированной на носители, в процессе его выдачи руководителю, сотруднику и прием от них носителя.

Следовательно, до начала составления черновика конфиденциального документа должен быть выполнен ряд принципиально важных технологических этапов обеспечения сохранности секретов организации, которые дают возможность в будущем свести к минимуму риск утраты конфиденциальной информации, документирование которой пока только предполагается.

2.7. Санкционирование изготовления и составление текста конфиденциального документа

Составление текста в ценных конфиденциальных документах обычно централизуется на уровне руководства фирмы. На любых черновика, вариантах, редакциях конфиденциальных документов (в том числе электронных), относящихся к

ним материалах, записях, записках и т.п. Обязательно и заблаговременно проставляется гриф конфиденциальности.

Говоря о технологии подготовки к документированию и документировании конфиденциальной информации, необходимо отметить наличие трех специфических особенностей (дополнительных этапах), необходимых для обеспечения заблаговременного сохранения в тайне содержания создаваемого документа: получение разрешения на составление документа, присвоение будущему документу определенного уровня грифа конфиденциальности и предварительный учет того носителя, на котором этот документ будет составляться.

Следующая, специфическая особенность, состоит в том, что ни один проект конфиденциального документа не может быть изготовлен с черновика и обрести статус правомерно документированной информации без дополнительной санкции (письменного разрешения) полномочного должностного лица организации.

2.8. Учет и изготовление конфиденциального документа

Следующее и, пожалуй, наиболее существенное документирование конфиденциальной информации, касающееся уже непосредственно технологических процедур изготовления самого документа, состоит в централизованном учете/регистрации - присвоении учетного номера проекту будущего документу.

Учету подлежат черновики всех конфиденциальных документов, независимо от места их составления и последующего изготовления проекта документа. Обязательно учитываются черновики подготовленных конфиденциальных подготовленных документов, факсов. Ответным документам присваивается новый учетный номер.

В случаи, когда сотрудник организации имеет разрешение на самостоятельное изготовление конфиденциальных документов, перед выполнением этого этапа он обязан передать черновик для учета. После регистрации черновик возвращается.

Как видно, черновик и проект будущего документа постоянно находиться под контролем. Этим в определенной мере обеспечивается сохранность информации,

которую руководство фирмы решило зафиксировать на том или ином типе носителя. Если открытые документы регистрируются только после их подписания или утверждения руководителя, то конфиденциальные документы - до изготовления проекта документа с черновика.

Процесс превентивного, предупредительного контроля за конфиденциальном документооборот и технологическая реализация этого процесса входят обязательной основной частью в структуру системы защиты информации от санкционированного доступа к информации постороннего лица и утраты носителя или конфиденциальности информации.

Целью этапа изготовления конфиденциального документа является перепечатывание черновика документа и создания оформленного в соответствии с государственным стандартом оригинала проекта документа, предназначенного по окончанию этапа издания стать подлинником документа.

Основная масса проекта типовых по содержанию конфиденциальных документов может с разрешением руководителя организации изготавливаться децентрализовано руководителями и сотрудниками фирмы непосредственно на рабочих местах при наличии специального защитного оборудования в их кабинетах и с соблюдением общего порядка учета этих документов.

При этом следует помнить, что этим лицам не разрешается передавать черновики документов для печати другим сотрудникам и подразделениям и не имеющих разрешения выполнять подобную работу. Изготовление конфиденциальных документов осуществляется только на выделенных для этих целей компьютерах и принтерах. Эти средства должны находиться под контролем руководителей структурных подразделений и специалистов в службе безопасности.

Конфиденциальные документы могут копироваться и тиражироваться с помощью соответствующей организационной техники и с соблюдением действующих требований по защите информации составляющую коммерческую тайну и сохранности всех сопровождающих этот процесс промежуточных носителей. Копирование и тиражирование конфиденциальных документов всегда санкционирует-

ся руководителем с проставлением необходимых записей в учетной форме основного документа и основных документов и отметке об этом в канцелярии.

2.9. Издание конфиденциального документа

При издании конфиденциальных документов должны быть решены следующие задачи обеспечения защиты документооборота:

1. Предупреждения ознакомления с документов руководителей и сотрудников, не имеющих служебного отношения к данному документу;
2. Предупреждения утраты документа и его частей, элементов текста в процессе передачи документов при издании;
3. Перекрытия визуальных и акустических каналов в процессе обсуждения с руководителями и сотрудниками содержания документа.

Издание документа включает в себя следующие последовательно выполняемые процедуры

1. Заключительное корректирование текста и подготовка документа к изданию;
2. Итоговое внутреннее согласование документа;
3. Внешнее согласование документа;
4. Подписание документа руководителем;
5. Регистрация документа в канцелярии.

Если в процессе визирования или подписания проекта документа принимаются решения об изменении уровня грифа конфиденциальности, то такое изменение должно быть срочно внесено во все экземпляры документа, черновик, редакции документа, учетные формы и описи.

Следовательно, документирование конфиденциальных сведений - изготовления конфиденциальных документов - сопровождается рядом специфических технологических этапов, необходимых для решения задач обеспечения сохранностей всех носителей и конфиденциальности документированной информации. Иной

порядок изготовления конфиденциальных документов неминуемо приведет к утрате секретов организации.

2.10. Вывод по второй главе

Таким образом, организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации, а также совокупность правовых норм и требований, устанавливаемых собственником информации с целью обеспечения регламентированного использования сотрудниками доверенных им ценных сведений, необходимых для выполнения служебных обязанностей.

Рассмотрены основные вопросы, касающиеся конфиденциального документооборота: дано понятие, определена цель и принципы его организации, сформулированы правила конфиденциального документооборота, выявлены основные угрозы и риски конфиденциального документооборота.

3. ПРЕДВАРИТЕЛЬНОЕ ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКОЙ СИСТЕМЫ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

3.1. Основные понятия ИСУБД CronosPro

ИСУБД Cronos имеет некоторый уникальный функционал в сравнении с другими СУБД что в свою очередь добавляет новые понятия и определения при работе с Cronos.

Банк данных – это система уникальным образом структурированных данных, главной его задачей является их накопление и анализ. В банке данных отображается некоторая часть предметной области ИСУБД. Поэтому создание банка направленно не на решение узконаправленных задач, а для универсального использования информации в определенной тематике

Недостатком привычных информационных систем, используемых для сбора информации, например, картотека, является трата большого количества времени на добавление и последующий поиск информации, тем более если информация охватывает широкую предметную область. Для исключения некорректности ввода данных, часто приходится копировать одну и те де данные. А анализ и процесс формирования отчетов в таком случае очень длителен и требует много сил. А в случае выявление ошибок допущенных на начальных этапах, сотруднику приходится исправлять все последующие результаты работы.

Описанные трудности работы с привычными нами информационными системами указывают на отсутствие контроля при вводе информации и негибкость использования всей системы в целом.

Таким образом, банк данных становится лучшей альтернативой любой картотеке. Его главной особенностью является облегчение работы с большими потоками информации. При этом гарантируются выполнение требований к информационным системам, такие как:

1. Полнота;
2. Достоверность;

3. Своевременность;
4. И другие.

3.1.1. Базы данных, записи, поля и значения

База данных – небольшая самостоятельная часть банка данных. Все данные в ИСУБД Cronos хранятся именно в базах данных. Поэтому основной банка данных является база данных. Совокупность связей и полей базы данных составляют структуру банка данных.

База данных описывает некоторый реальный объект. В нашем случае, одним из объектов банка данных будут являться сотрудники. Информация о документах будет добавляться и хранится согласно структуре нашей базы данных. Тем самым, структура базы данных это описание хранения накапливаемых данных.

Если привести пример с картотекой, то данные о конкретном лице(сотруднике) будут находится в отдельной картотеке, где каждая карточка соответствовала бы одному сотруднику. Шаблон карточки будет однотипен, везде были бы данные о должности, фамилии и имени сотрудника, даты устройства его на работу и.т.д. В этом примере картотека соответствует базе данных а шаблон карточки, её поля – соответствуют структуре базы данных.

3.1.2. Запись базы данных

Все базы данных состоят из записей, соответствуя карточкам в картотеке. В картотеке одна карточка описывает отдельного взятого сотрудника, так и в базе данных запись описывает одного сотрудника.

Также следует отметить особенность ИСУБД CRONOS что каждая запись в базе имеет уникальный системный номер, номер создается системой автоматически и служит для того чтобы система могла отличить записи друг от друга. Пользователь ИСУБД может узнать этот номер и использовать его(например для поиска записи) но не может его изменять или задавать.

3.1.3. Поле записи

Поле записи – это часть структуры, обязательная составляющая каждой записи. Любая запись базы данных будет содержать одинаковый набор полей. В момент проектирования базы данных и создания её структуры, принимается решение о том, какие поля будет содержать база данных и соответственно, какие поля будут у каждой записи. Если база данных создается для накопления информации о сотрудниках, то она будет содержать следующую информацию:

1. Фамилия;
2. Имя;
3. Отчество;
4. Дата рождения;
5. Должность;
6. И.т.д.

Это означает что запись базы данных будет содержать такие же поля.

Значение поля – это определенные данные, содержащиеся в каждом поле. Например, в нашем случае в базе данных СОТРУДНИКИ каждая запись будет соответствовать одному сотруднику и у записи будет поле ФАМИЛИЯ, которая содержит значение фамилии этого сотрудника.

Если представить базу данных виде таблицы, то записи базы данных соответствуют строкам таблицы, названия столбцов соответствуют названиям полей базы а ячейка таблицы содержит значение поля.

3.1.4. Свойства полей

Первоочередным свойством поля базы данных является определение типа поля. Оно определяет, какой тип данных будет хранится в данном поле, что в свою очередь определяет возможный перечень операций над этим полем. В нашей информационно- аналитической системе будет использовано множество различных свойств и типов полей. Основным типом поля будет являться ТЕКСТОВЫЙ.

Явное обозначение поля требуется для того, чтобы система знала как хранить и обрабатывать вводимые пользователем данные а в случае некорректного ввода могла указать пользователю на его ошибку.

Еще одним из важных свойств поля в ИСУБД Cronos является определение, сколько значений одновременно может хранить в себе поле. Данное поле может быть МНОЖЕСТВЕННЫМ, если требуется хранить сразу несколько значений.

Например поле ДОЛЖНОСТЬ в базе данных СОТРУДНИКИ имеет свойство МНОЖЕСТВЕННОЕ т.к. сотрудник может иметь более одной должности.

Данное свойство в некоторой мере решает проблему дублирования информации. Если сотрудник имеет две должности: “Начальник структурного подразделения” и “член комиссии по уничтожению документов”, в ИСУБД Cronos не придется создавать две одинаковые записи о сотруднике с одной только разницей в его должности.

Также в своей информационно – аналитической системе я буду использовать важной свойство поля, которое означает, обязательно ли заполнение данного поля при создании новой запили или нет. Для этого при формировании структуры базы данных требуется определить, является данное поле ОБЯЗАТЕЛЬНЫМ или нет.

3.1.5. Словарный банк данных

Одной из важных уникальных функций данной ИСУБД является возможность подключения СЛОВАРНЫХ баз данных. Для лучшего понимая следует привести пример на основе нашей системы конфиденциального документооборота.

Если бы мы использовали картотеку, то при заполнении поля ДОЛЖНОСТЬ разными сотрудниками можно получить разные значения поля при написании одной и той же должности, в первую очередь это возникает при отсутствии стандартизации определений используемых для заполнения поля, в нашем случае - списка должностей. Не исключены и простые орфографические ошибки при написании. К сожалению, проблемы данного рода будут присутствовать и не только в бумажной картотеке, но так же и в электронных информационных – системах.

Для минимизации рисков совершения подобных ошибок в ИСБУД Cronos введено понятие словарного баз данных. Словарная база описывает все возможные значения определенного поля базы данных, описание которого требует однозначности и точности ввода. Таким образом поле ДОЛЖНОСТЬ будет сводится к выбору должности из заранее описанного списка. Данный список нужно предварительно создать и заполнить. В нашей работе иногда я буду использовать понятие СЛОВАРЬ.

3.1.6. Использование запросов для поиска данных

Накапливание информации становится бессмысленным если не планируется её обрабатывать. ИСУБД Cronos обеспечивает быструю работу и эффективный поиск данных с помощью специальной конструкции формирования поисковых запросов.

Запрос – это основной инструмент для выборки, изменения и поиска данных в соответствии с определенными требованиями. При помощи запросов можно выбрать только интересующие нас данные в удобном для нас виде.

3.2. Постановка задачи

Основная задача организации информационно-аналитической системы на предприятии является обеспечение качественного контроля и предупреждения возможных ошибок в процессе конфиденциального документооборота.

Корректно спроектированный банк данных дает возможность быстрого и легкого доступа к имеющейся информации. Соответственно, если банк данных спроектирован верно, то времени и человеческих ресурсов при работе с информацией будет затрачено минимально возможное количество а результат работы будет лучше. Иначе может возникнуть ситуация когда в банке данных будет множество ошибок которые нелегко исправить.

Тем самым, при проектировании банка данных мы должны учитывать выполнение всех требований, предъявляемых к информационной системе перечисленных в главе 1.

3.3. Описание предметной области

Нам требуется создать банк данных для использования его в подразделении, отвечающем за конфиденциальное делопроизводство. В банке будет накапливаться информация о лицах получивших доступ к конфиденциальным документам, в первую очередь это будут сотрудники предприятия. Но ознакомится с документом, могут также и государственные структуры при различных проверках. Наша система должна учитывать такую возможность. Кроме накопления информации о лицах, в системе будут храниться реквизиты документов. Накопление информации о наличии связей между лицом и документом является одной из важнейшей функции информационно-аналитической системы.

Следует отметить, что все поступающие данные должно автоматически проверятся и минимизировать риск ввода ошибочных данных. Данный банк создается для того, чтобы максимально упростить поиск и анализ информации о определённом документе и/или лице и наличии связей между ними. С его помощью можно быстро найти сотрудника, который последний ознакамливался с документом. Или найти все документы, не приобщенные в дело и не имеющие статус отправленных.

Также стоит понимать что размеры банка будут постоянно расти т.к в него регулярная добавляется информация и со временем размер может достигать тысячи или даже десятки тысяч записей, соответственно поиск и анализ данных банка всегда должен быть быстрым и простым для сотрудника.

Перед этапом проектирования следует определить основные объекты, используемые в системе конфиденциального документооборота:

1. Лицо, в том числе сотрудники, бывшие сотрудники предприятия и лица ознакомившиеся с конфиденциальной информацией;

2. Документ. Реквизиты документа, его тип и прочее;
3. Внешние электронные накопители;
4. Действие. Регистрация различных действий, относящихся к конфиденциальному документообороту.

3.4. Определение баз данных и их полей

На данном этапе нужно определить, какие базы данных будут находится в составе банка, определить названия и мнемокды. В соответствии с основными объектами, перечисленным выше наша первая база данных будет называться ЛИЦА.

В ее состав буду входить следующие поля:

1. Имя;
2. Фамилия;
3. Отчество;
4. Пол;
5. Дата рождения;
6. Дата приема на работу;
7. Должность;
8. Исполнитель документов/съемный носителей;
9. Был ознакомлен;
10. Действующий.

Поля 4,7, являются словарными и имеют значения МУЖСКОЙ/ЖЕНСКИЙ и список должностей организации соответственно. Поле должность является множественным что дает возможность указать несколько должностей для одного сотрудника. 8,9 поля являются сложными связаны с записями других баз.

На рисунке 1 предоставлены настройки структуры базы данных ЛИЦА.

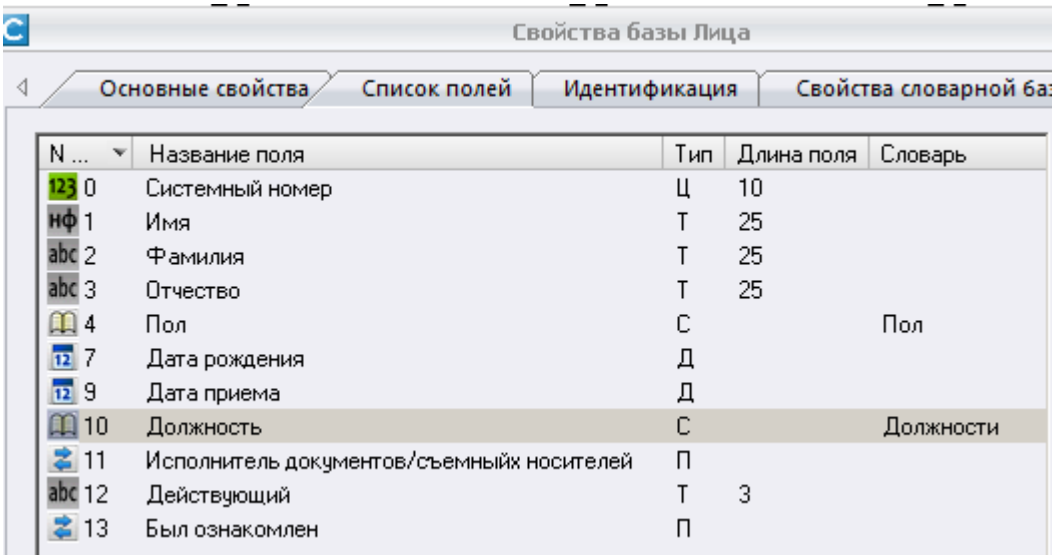


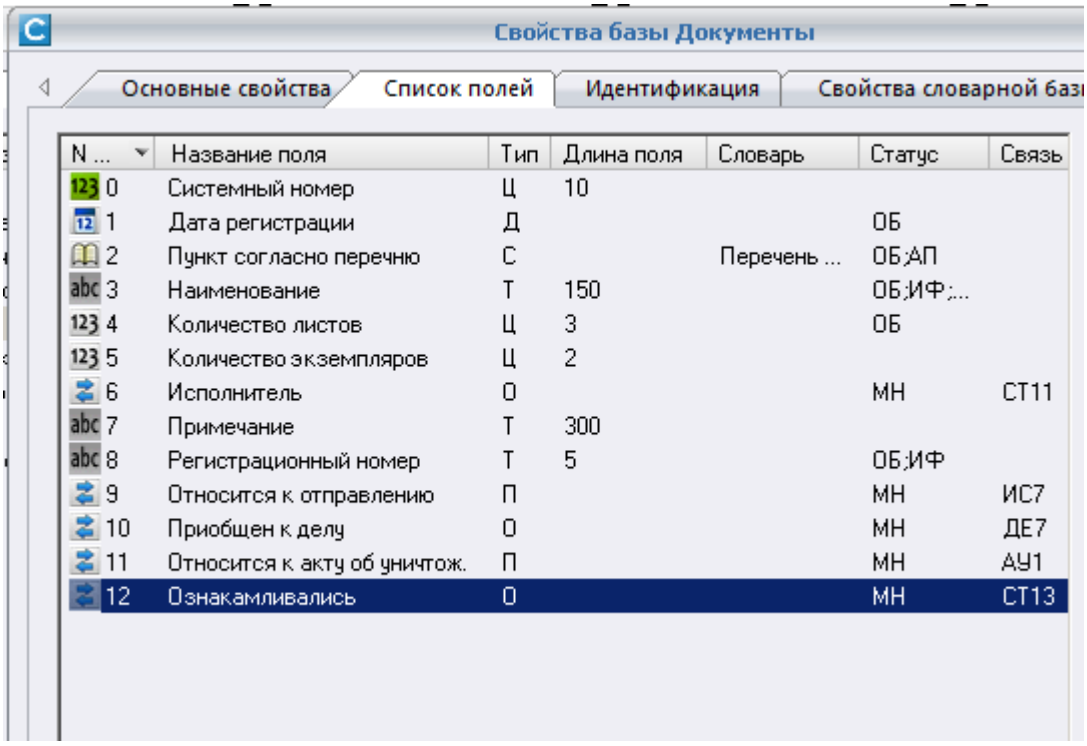
Рисунок 1. Структура базы данных ЛИЦА

Определив структуру базы ЛИЦА следует перейти к следующему информационному объекту нашей информационно – аналитической системе. База данных ДОКУМЕНТ требуется для регистрации конфиденциальных документов, при регистрации нового документа требуется указать его реквизиты. Структура базы имеет следующие поля:

1. Дата регистрации;
2. Пункт согласно перечня;
3. Наименование;
4. Количество листов;
5. Количество экземпляров;
6. Исполнитель;
7. Примечание;
8. Регистрационный номер;
9. Относится к отправлению;
10. Приобщен к делу;
11. Относится к акту об уничтожении;
12. Ознакамливались.

Поле 2 имеет словарный тип и относится к словарю ПЕРЕЧЕНЬ ДОКУМЕНТОВ. Поле 6 связано с полем 8 базы ЛИЦО. Также поле 12 связано с полем 9 базы

ЛИЦО. Поля 9,10,11 имеют тип сложное и имеют связи с другими базами данных. На рисунке 2 предоставлены настройки структуры базы данных ДОКУМЕНТ.



N ...	Название поля	Тип	Длина поля	Словарь	Статус	Связь
0	Системный номер	Ц	10			
1	Дата регистрации	Д			ОБ	
2	Пункт согласно перечню	С		Перечень ...	ОБ;АП	
3	Наименование	Т	150		ОБ;ИФ;...	
4	Количество листов	Ц	3		ОБ	
5	Количество экземпляров	Ц	2			
6	Исполнитель	О			МН	СТ11
7	Примечание	Т	300			
8	Регистрационный номер	Т	5		ОБ;ИФ	
9	Относится к отправлению	П			МН	ИС7
10	Приобщен к делу	О			МН	ДЕ7
11	Относится к акту об уничтож.	П			МН	АУ1
12	Ознакамливались	О			МН	СТ13

Рисунок 2. Структура базы данных ДОКУМЕНТЫ

Далее стоит описать поля объекта ВНЕШНИЕ ЭЛЕКТРОННЫЕ НАКОПИТЕЛИ. Данная база имеет следующие поля:

1. Регистрационный номер;
2. Тип носителя;
3. Объем памяти;
4. Заводской серийный номер;
5. Исполнитель;
6. Дата возврата;
7. Относится к отправлению;
8. Относится к акту об уничтожении;
9. Ознакамливались.

Поле 2 имеет словарный тип. Поля 5,8,9,10 являются сложными. На рисунке 3 предоставлены настройки структуры базы данных ВНЕШНИЕ ЭЛЕКТРОННЫЕ НАКОПИТЕЛИ.

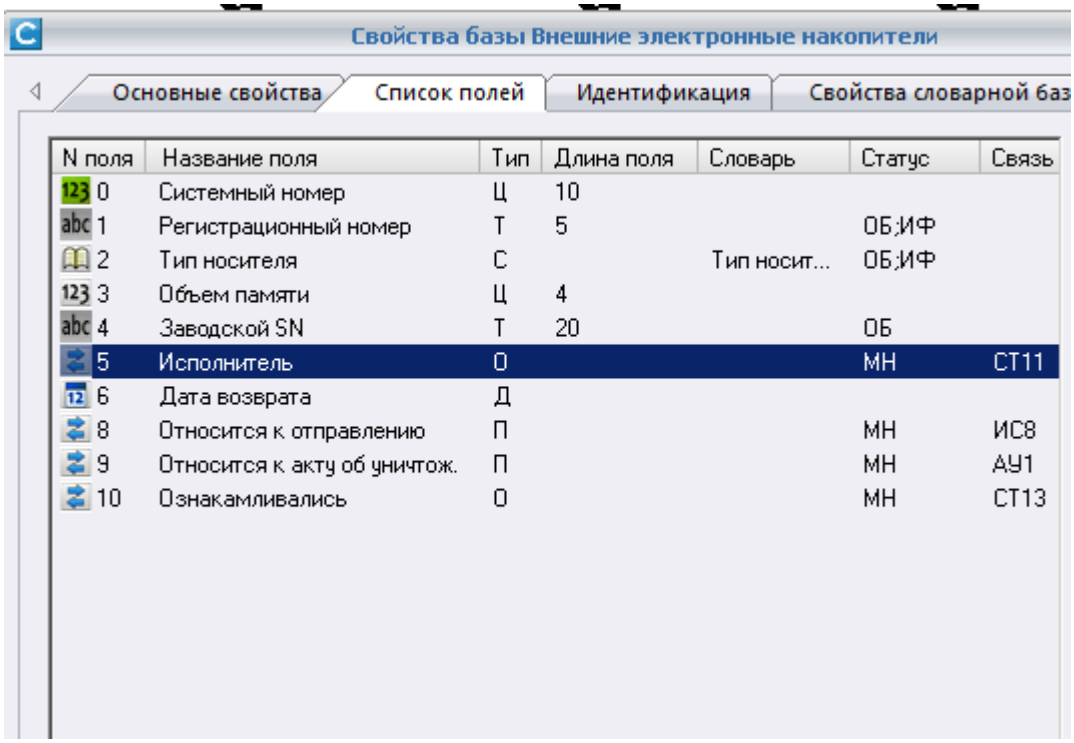


Рисунок 3. Структура базы данных ВНЕШНИЕ ЭЛЕКТРОННЫЕ НАКОПИТЕЛИ

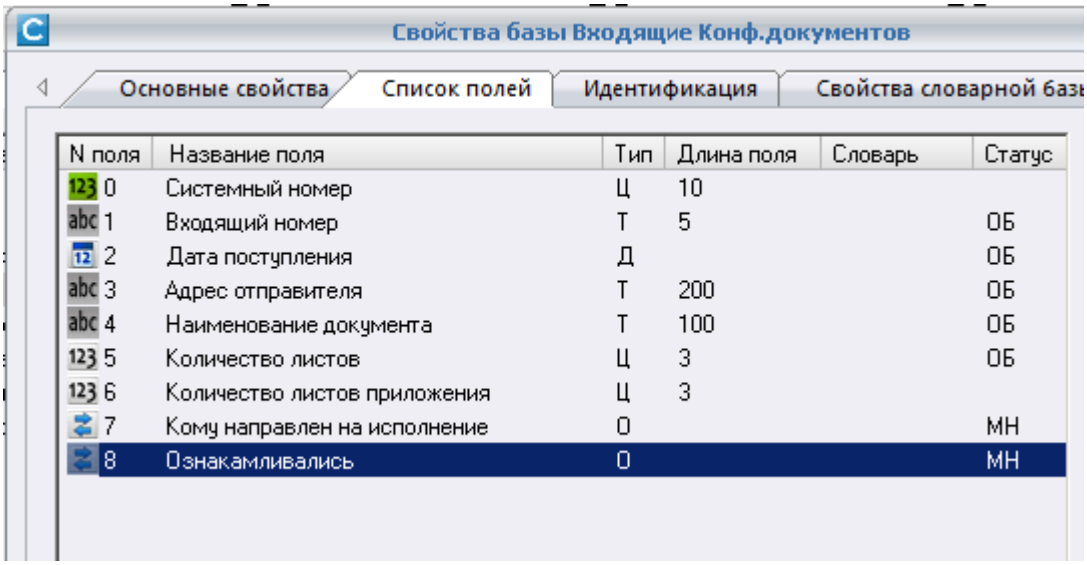
Описав структуру объекта ДОКУМЕНТ, следует описать вспомогательные базы данных, относящиеся к данному объекту.

База данных ВХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ содержит информацию о входящей конфиденциальной корреспонденции. В её состав входят такие поля:

1. Входящий номер;
2. Дата поступления;
3. Адрес отправителя;
4. Наименование документа;
5. Количество листов;
6. Количество листов приложения;
7. Кому направлен на исполнение;
8. Ознакамливались.

Тем самым данная структура полностью описывает все реквизиты входящей корреспонденции. Поля 7, 8 являются сложными. Словарных полей в предложен-

ной структуре нет. На рисунке 4 предоставлены настройки структуры базы данных ВХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ.



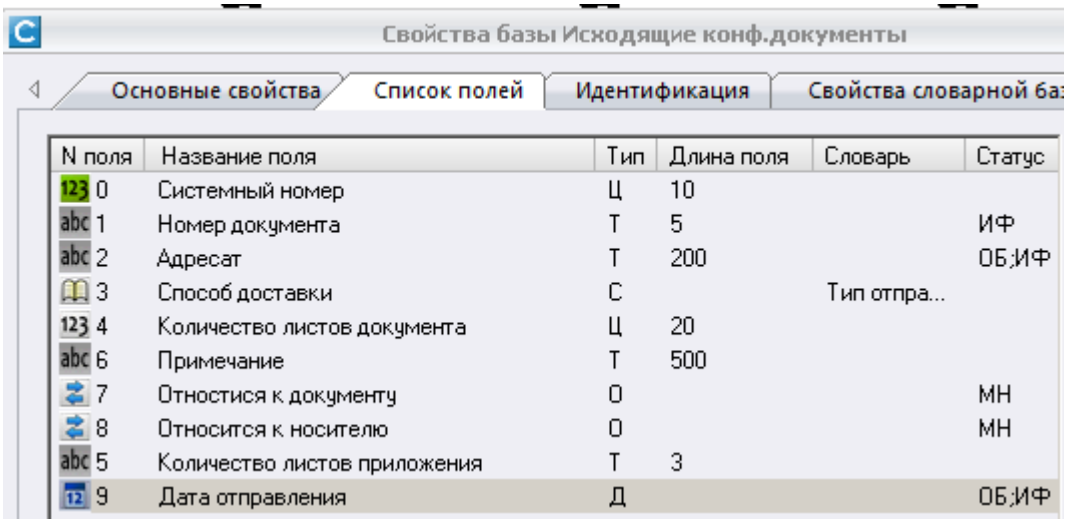
N поля	Название поля	Тип	Длина поля	Словарь	Статус
0	Системный номер	Ц	10		
1	Входящий номер	Т	5		ОБ
2	Дата поступления	Д			ОБ
3	Адрес отправителя	Т	200		ОБ
4	Наименование документа	Т	100		ОБ
5	Количество листов	Ц	3		ОБ
6	Количество листов приложения	Ц	3		
7	Кому направлен на исполнение	О			МН
8	Ознакамливались	О			МН

Рисунок 4. Структура базы данных ВХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ

Описав базу данных входящей корреспонденции не стоит забывать и о том, что также возможна отправка документ из предприятия во вне. Для контроля исходящей корреспонденции создана вспомогательная база ИСХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ. База состоит из полей:

1. Номер документа;
2. Адресат;
3. Способ доставки;
4. Количество листов документа;
5. Примечание;
6. Относится к документу;
7. Относится к носителю;
8. Количество листов приложения;
9. Дата отправления.

Поле 3 имеет словарный тип. Поля 7, 8, 9 имеют сложный тип. На рисунке 5 предоставлены настройки структуры базы данных ИСХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ.



N поля	Название поля	Тип	Длина поля	Словарь	Статус
0	Системный номер	Ц	10		
1	Номер документа	Т	5		ИФ
2	Адресат	Т	200		ОБ;ИФ
3	Способ доставки	С		Тип отпра...	
4	Количество листов документа	Ц	20		
6	Примечание	Т	500		
7	Относится к документу	О			МН
8	Относится к носителю	О			МН
5	Количество листов приложения	Т	3		
9	Дата отправления	Д			ОБ;ИФ

Рисунок 5. Структура базы данных ИСХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ

Еще одной важной особенностью для объекта документ является возможность приобщать документ к делу, для этого создана отдельная база ДЕЛА. Ниже перечислены её поля:

1. Номер дела;
2. Дата выдачи;
3. Наименование дела;
4. Кому выдано;
5. Дата возврата;
6. Отметка о том, выдана ли сотруднику пустая карта;
7. Приобщенные документы;
8. Акт об уничтожении.

Поля 4, 7 и 8 являются сложными и связаны с другими базами. На рисунке 6 предоставлены настройки структуры базы данных ДЕЛА.

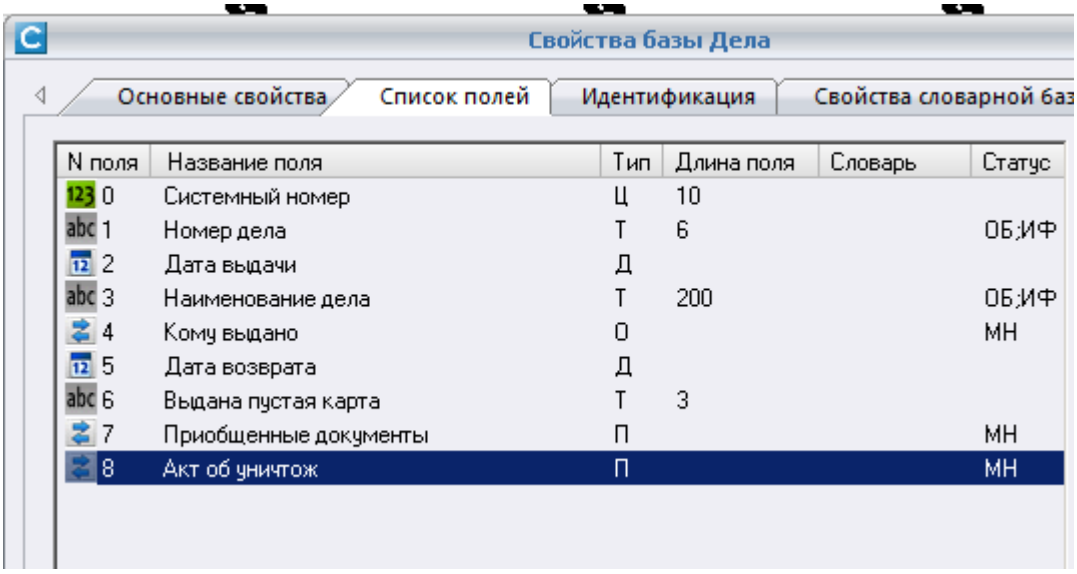


Рисунок 6. Структура базы данных ДЕЛА

В настоящее время, в процессе работы предприятия создается множество различных документов. Правильное и своевременно уничтожение документов является довольно важным моментом в делопроизводстве.

Для контроля деятельности по уничтожению документов в процессе конфиденциального документооборота, в банке отведена специальная база данных, именуемая АКТЫ ОБ УНИЧТОЖЕНИИ. База имеют следующие поля:

1. Относится к документу/делу;
2. Номер акта;
3. Примечание.

Структура данной базы достаточно проста, сложным является только поле 1. На рисунке 7 предоставлены настройки структуры базы данных АКТЫ ОБ УНИЧТОЖЕНИИ.

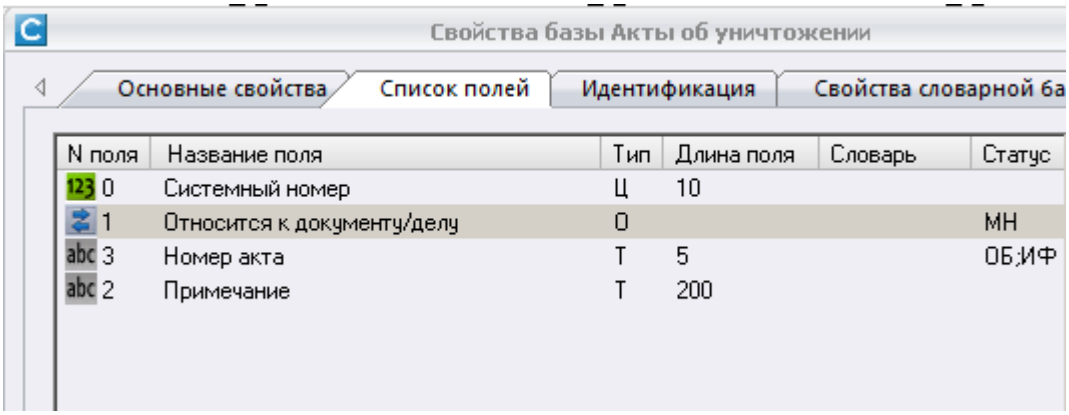


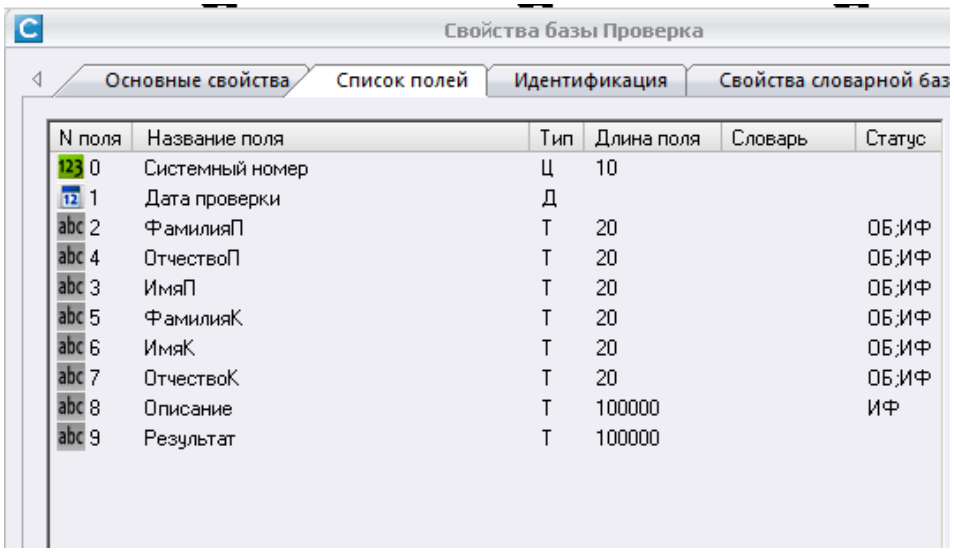
Рисунок 7. Структура базы данных АКТЫ ОБ УНИЧТОЖЕНИИ

Также не стоит забывать, что одной из основных задач контроля является оценка качества и своевременности выполнения работы. В нашем случае это оценка соответствия сотрудниками требований инструкции по конфиденциально-

му делопроизводству. Поэтому для хранения результатов различных проверок создана база данных ДЕЙСТВИЕ. База состоит из полей:

1. Дата ДЕЙСТВИЯ;
2. Фамилия проверяемого;
3. Имя проверяемого;
4. Отчество проверяемого;
5. Фамилия ответственного;
6. Имя того ответственного;
7. Отчество того ответственного;
8. Описание действия;
9. Результат действия.

Структура базы проста. На рисунке 8 предоставлены настройки структуры базы данных ДЕЙСТВИЕ.



N поля	Название поля	Тип	Длина поля	Словарь	Статус
0	Системный номер	Ц	10		
1	Дата проверки	Д			
2	ФамилияП	Т	20		ОБ;ИФ
4	ОтчествоП	Т	20		ОБ;ИФ
3	ИмяП	Т	20		ОБ;ИФ
5	ФамилияК	Т	20		ОБ;ИФ
6	ИмяК	Т	20		ОБ;ИФ
7	ОтчествоК	Т	20		ОБ;ИФ
8	Описание	Т	100000		ИФ
9	Результат	Т	100000		

Рисунок 7. Структура базы данных ПРОВЕРКА

Таким образом в этой части главы были определены основные базы данных, и структура и типы полей.

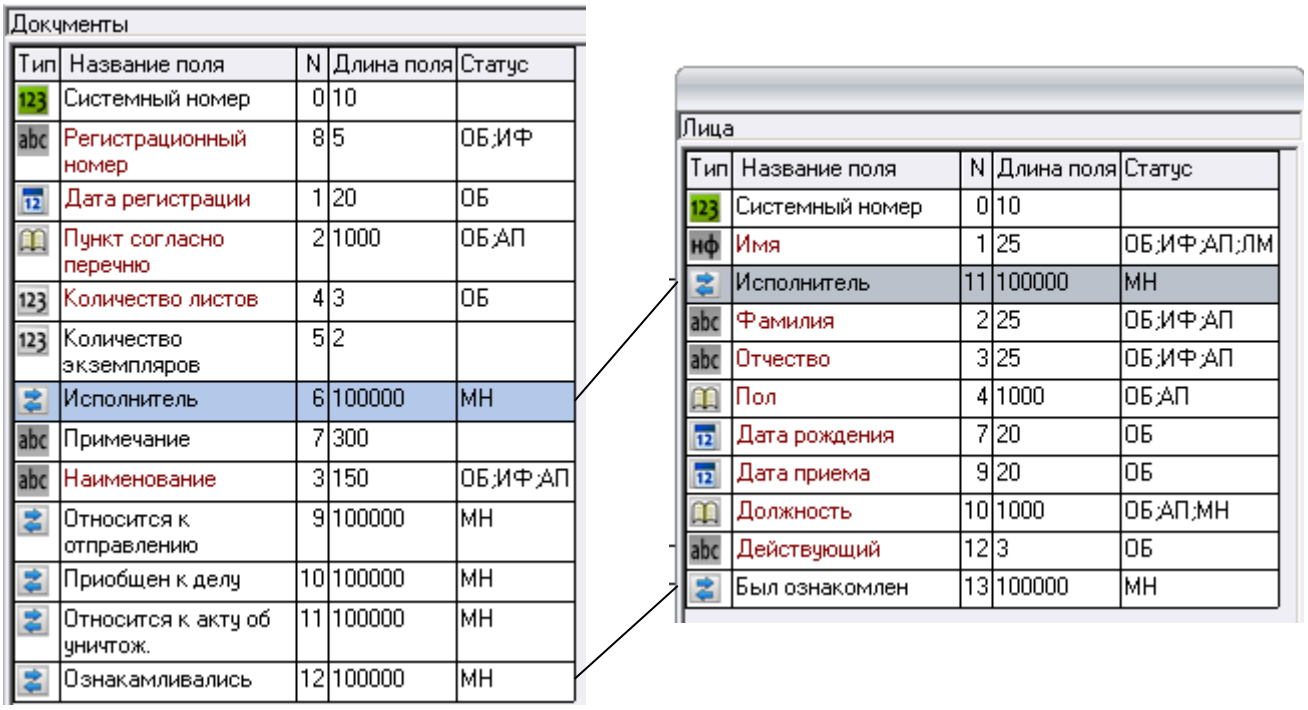
3.5. Определение связей между базами данных

Главным преимуществом качественной структуры банка данных является отсутствие избыточности (повторения) информации. Для этого, ранее, мы распределили информацию на несколько отдельных тематических баз данных. В ИСУБД CronosPro мы будем использовать особенный способ сбора данных, разделенных на различные базы – это осуществляется путем создания сложных полей и установлением связей между полями различных баз данных.

Как уже говорилось ранее, логически систему конфиденциального делопроизводства можно разделить на несколько основных объектов. Эти объекты описаны в виде одной или нескольких таблиц и связаны между собой с помощью сложных полей.

Первым объектом являются лица, когда-либо получавшие доступ к документам, содержащим конфиденциальную информацию. Соответственно база ЛИЦА должна иметь связь по полю с базой ДОКУМЕНТЫ. В первую очередь нас могут интересовать, какие документы находятся у сотрудника на руках и с какими документами за все время работы был ознакомлен сотрудник.

Для этого в базе ЛИЦА созданы поля ИСПОЛЬНИТЕЛЬ и БЫЛ ОЗНАКМЛЕН. Данные поля имеют множественные связи с базами данных, относящихся к объекту ДОКУМЕНТ. В первую очередь связь с базой ДОКУМЕНТ по полям ИСПОЛЬНИТЕЛЬ и ОЗНАКАМЛИВАЛИСЬ соответственно. Это означает что у любого сотрудника будут связи с документами, которые в данный момент находятся у сотрудника и с которыми сотрудник или лицо были ознакомлены. Связь является множественной т.к. лицо единовременно, может, хранить у себя несколько конфиденциальных документов и поле ИСПОЛНИТЕЛЬ будет иметь множество связей с записями о различных документах. На рисунке 8 изображена схема связи между базой ЛИЦО и ДОКУМЕНТ.



Документы

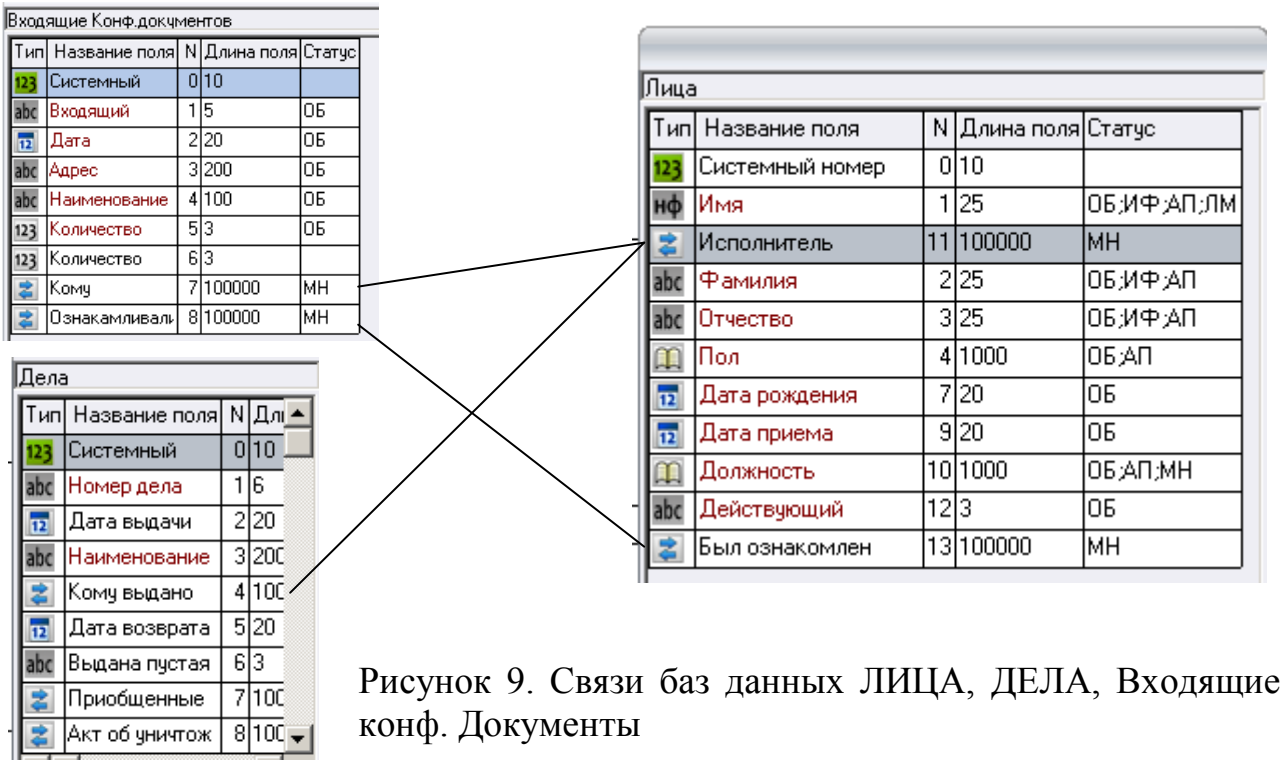
Тип	Название поля	N	Длина поля	Статус
123	Системный номер	0	10	
abc	Регистрационный номер	8	5	ОБ;ИФ
12	Дата регистрации	1	20	ОБ
	Пункт согласно перечню	2	1000	ОБ;АП
123	Количество листов	4	3	ОБ
123	Количество экземпляров	5	2	
	Исполнитель	6	100000	МН
abc	Примечание	7	300	
abc	Наименование	3	150	ОБ;ИФ;АП
	Относится к отправлению	9	100000	МН
	Приобщен к делу	10	100000	МН
	Относится к акту об уничтож.	11	100000	МН
	Ознакамливались	12	100000	МН

Лица

Тип	Название поля	N	Длина поля	Статус
123	Системный номер	0	10	
нф	Имя	1	25	ОБ;ИФ;АП;ЛМ
	Исполнитель	11	100000	МН
abc	Фамилия	2	25	ОБ;ИФ;АП
abc	Отчество	3	25	ОБ;ИФ;АП
	Пол	4	1000	ОБ;АП
12	Дата рождения	7	20	ОБ
12	Дата приема	9	20	ОБ
	Должность	10	1000	ОБ;АП;МН
abc	Действующий	12	3	ОБ
	Был ознакомлен	13	100000	МН

Рисунок 8. Связи базы данных ЛИЦО и ДОКУМЕНТ

Не стоит забывать, что ранее мы определили еще несколько баз, описывающих документы. Это базы ВХОДЯЩИЕ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ, ДЕЛА. Данные базы также будут связаны по полю ИСПОЛЬНИТЕЛЬ и БЫЛ ОЗНАКОМЛЕН. Визуальное представление связей изображено на рисунке 9.



Входящие Конф.докуметов

Тип	Название поля	N	Длина поля	Статус
123	Системный	0	10	
abc	Входящий	1	5	ОБ
12	Дата	2	20	ОБ
abc	Адрес	3	200	ОБ
abc	Наименование	4	100	ОБ
123	Количество	5	3	ОБ
123	Количество	6	3	
	Кому	7	100000	МН
	Ознакамливали	8	100000	МН

Дела

Тип	Название поля	N	Дл
123	Системный	0	10
abc	Номер дела	1	6
12	Дата выдачи	2	20
abc	Наименование	3	200
	Кому выдано	4	100
12	Дата возврата	5	20
abc	Выдана пустая	6	3
	Приобщенные	7	100
	Акт об уничтож	8	100

Лица

Тип	Название поля	N	Длина поля	Статус
123	Системный номер	0	10	
нф	Имя	1	25	ОБ;ИФ;АП;ЛМ
	Исполнитель	11	100000	МН
abc	Фамилия	2	25	ОБ;ИФ;АП
abc	Отчество	3	25	ОБ;ИФ;АП
	Пол	4	1000	ОБ;АП
12	Дата рождения	7	20	ОБ
12	Дата приема	9	20	ОБ
	Должность	10	1000	ОБ;АП;МН
abc	Действующий	12	3	ОБ
	Был ознакомлен	13	100000	МН

Рисунок 9. Связи баз данных ЛИЦА, ДЕЛА, Входящие конф. Документы

Данные связи обеспечивают возможность получения полной информации о том, с какими документами ознакамливалось лицо. Тем не менее эта структура не учитывает возможности узнать какие внешние электронные накопители находятся у лица. Для этого между базой ВНЕШНИЕ ЭЛЕКТРОННЫЕ НАКОПИТЕЛИ и ЛИЦО требуется создать связь по полю ИСПОЛЬНИТЕЛЬ. Визуальное представление связей изображено на рисунке 10.

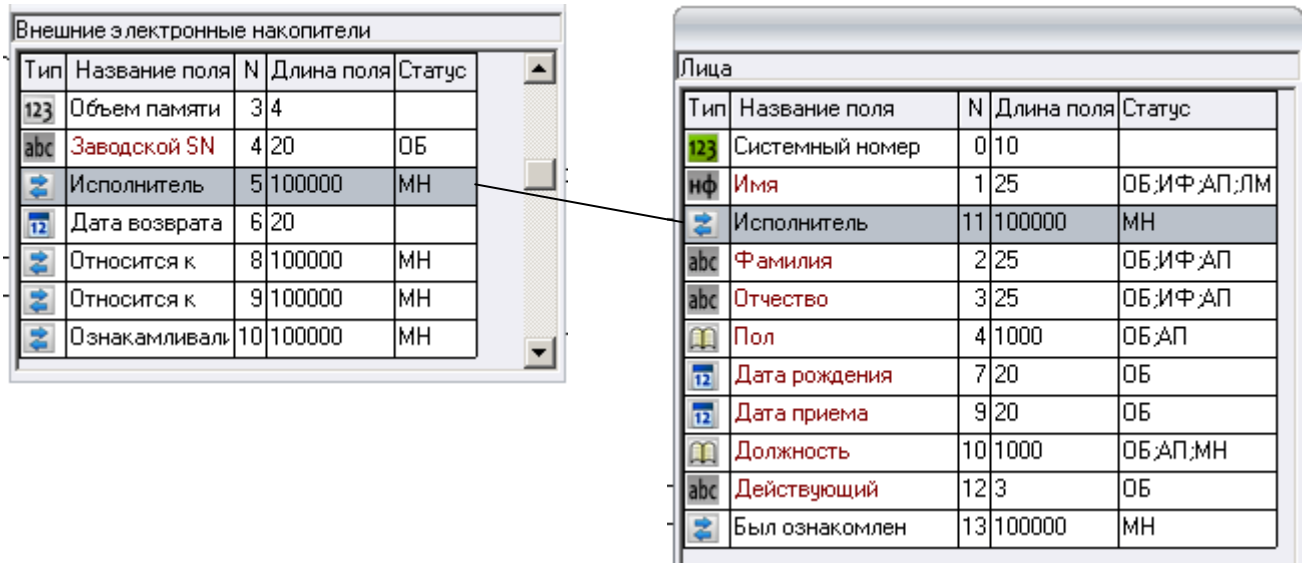


Рисунок 10. Связь баз ЛИЦА и ВНЕШНИЕЭЛЕКТРОННЫЕ НАКОПИТЕЛИ

С полной, более подробной структурой базы данных можно ознакомиться в приложении Б.

3.6. Создание форм для работы пользователя

В ИСУБД CronosPro для различного рода редактирования, ввода данных а также просмотра имеющихся записей применяются специально созданные оконные формы.

Формы обеспечивают быстрый удобный доступ к информации, хранящейся в одно или нескольких базах данных. Помимо этого, формы дают возможность разработчику использовать функционал данной ИСУБД не применяя стандартный интерфейс.

В нашей системе, основная работа пользователя по вводу, редактированию и просмотру данных будет осуществляться через специальные формы.

Для начала стоит определится с основными требованиями к возможностям системы, это даст понятие о том как должен выглядеть интерфейс формы. Первым будет работа с объектом ЛИЦО. Ниже перечислены основные задачи, которые будут решаться пользователем системе с помощью формы:

1. Создание нового лица;
2. Просмотр всех лиц, хранящихся в базе;
3. Поиск лица по реквизитам(фамилии и/или имя);
4. Редактирование данных записи;
5. Список документов, дел, внешних носителей находящихся в данный момент у лица;
6. Список документов, дел с которыми когда либо ознакамливалось лицо.

Стоит напомнить, что это далеко не все задачи, которые может решить система. Это лишь список задач, решение которых будет осуществляться с помощью дополнительно разработанных форм для упрощения взаимодействия пользователя с системой.

Пример разработанной формы изображен на рисунке 11.

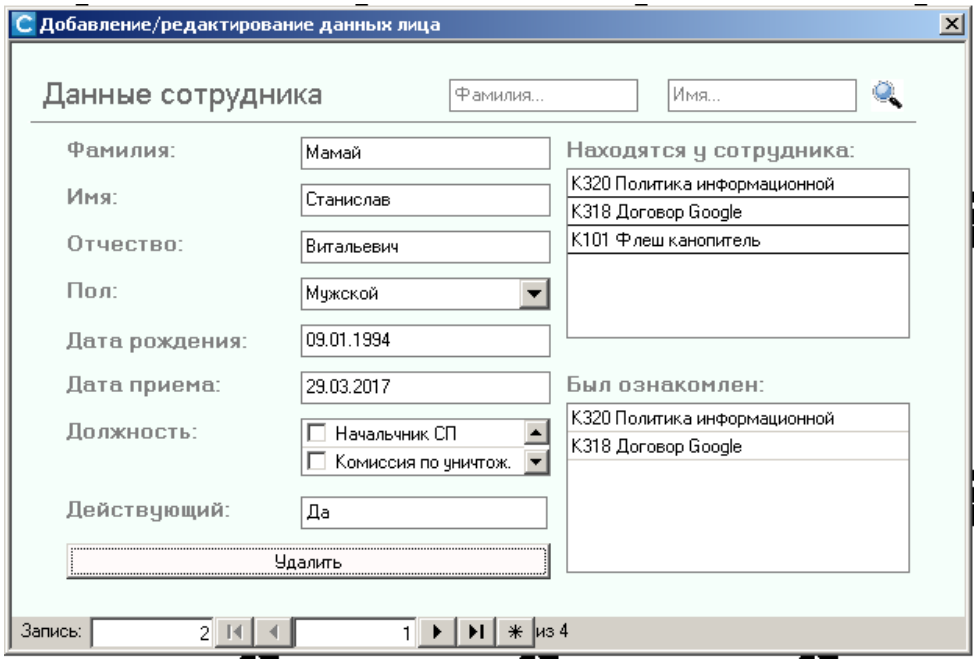


Рисунок 11. Пример формы ЛИЦА

Визуально форму можно разделить на несколько объектов:

1. Строка поиска
2. Основная рабочая область для ввода, редактирования и просмотра данных
3. Кнопки управления записями

Строка поиска – решает задачу поиска лица по заданным реквизитам, в нашем случае это Имя и Фамилия.

Основная рабочая область – позволяет пользователю системы быстро и легко редактировать, вводить и просматривать данные определенной записи базы данных и связанных с нею базами.

Кнопки управления записями – нужны для поочередного перехода между записями а также создания новой записи.

Таким образом, данная форма помогает решить основные задачи при работе с системой. Обработка действий пользователя в форме в ИСУБД CronosPro описывается с помощью языка Lua.

Для объекта ДОКУМЕНТ тоже следует создать несколько форм, которые будут решать следующие задачи:

1. Регистрация нового документа входящего, исходящего, внутреннего, в том числе и актов об уничтожении дел и актов о совершенных проверках;
2. Поиск требуемого документа по его реквизитам(номер документа);
3. Быстрый просмотр основной информации о документе;
4. Возможность редактирования данных о документе в том числе и сложных полей;

Формы упрощают работу пользователя с системой, но не решают всех требуемых задач. Важным элементом работы с системой является поиск информации с помощью сложных запросов, наша система должна быстро и в удобной для пользователя выводить следующую информацию:

1. Кто ознакамливался с документов за все время его существования;

2. Поиск всех документов, не приобщенных в дело и не являющихся отправленными во вне;

3. Все проверки, проведенные за определенный период времени;

4. Все проверки, касающиеся определенного сотрудника;

5. И другие.

Данная задача решается просто с помощью стандартного интерфейса ИСУБД CronosPro. С помощью шаблонов запросов. В нашей системе созданные основные шаблоны запросов, пользователю остается только выбрать нужный и запрос у казать основные параметры поиска.

3.7. Вывод по третьей главе

Во третьей главе были описаны основные понятия ИСУБД CronosPro. Проведено предпроектное обследование, описана структура банка данных. Проведен анализ требуемых задач, стоящих перед информационно – аналитической системой конфиденциального делопроизводства. Разработаны управляющие формы и сконфигурированная система для работы пользователя

Результатом третьей главы стала разработанная информационно - аналитическая система конфиденциального делопроизводства на базе ИСУБД CronosPro.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Введение

Главной целью безопасности жизнедеятельности является обеспечение безопасности и создание качественных условий для комфортной работы. Возможность осуществления трудовой деятельности в опасных, а иногда даже в чрезвычайно опасных условиях достаточно велика. Различные отклонения от допустимых условий деятельности сопровождаются воздействием негативных факторов на человека, что отрицательно влияет на производительность труда, ухудшает самочувствие, приводит к травмам и заболеваниям, а иногда и гибели людей. Также это вызывает отказы и аварии производственного оборудования.

Работа пользователя с информационно – аналитической системой конфиденциального делопроизводства производится с помощью средств вычислительной техники, нам необходимо обеспечить соответствие автоматизированного рабочего места сотрудника с действующими нормами стандартов безопасности жизнедеятельности.

4.1. Рекомендации по организации рабочего места пользователя

4.1.1. Требования к помещениям для размещения рабочего места

Работа с вычислительной техникой является неотъемлемым процессом трудовой деятельности и правильно спроектированное помещение, в котором будут находится рабочие места сотрудником, может качественно повысить уровень работоспособности.

В соответствии с СанПиН 2.2.2/2.4.1340-03 помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение;

2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации;

3. Не допускается размещение мест пользователей ПЭВМ во всех образовательных и культурно-развлекательных учреждениях для детей и подростков в цокольных и подвальных помещениях;

4. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 $м^2$;

5. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7 - 0,8; для стен - 0,5 - 0,6; для пола - 0,3 - 0,5;

6. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;

7. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.1.2. Требования к уровням шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Основными постоянными источниками шума могут являться автоматизированные рабочие станции и серверное оборудованием. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА. В соответствии с нормами, ограни-

чивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.1.3. Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03, есть следующие требования к освещению на рабочих местах:

1. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;

2. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения;

3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк;

4. Для освещения помещений с ПЭВМ следует применять светильники с зеркальными параболическими решетками, укомплектованными электронными пуско-регулирующими аппаратами (ЭПРА) ;

5. Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном рас-

положении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору;

6. Коэффициент пульсации не должен превышать 5%;

7. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.1.4. Общие требования к организации рабочих мест пользователей

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

1. При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;

2. Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом;

3. Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 - 2,0 м;

4. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 - 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;

5. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы;

6. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7;

7. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ;

8. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;

9. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений;

10. Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

11. Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм;

12. Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм;

13. Конструкция рабочего стула должна обеспечивать:

13.1.Ширину и глубину поверхности сиденья не менее 400 мм;

13.2.Поверхность сиденья с закругленным передним краем;

13.3.Регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 град, и назад до 5 град.;

13.4.Высоту опорной поверхности спинки 300 +-20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;

13.5.Угол наклона спинки в вертикальной плоскости в пределах +-30 градусов;

13.6.Регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм;

13.7.Стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50 - 70 мм;

13.8.регулировку подлокотников по высоте над сиденьем в пределах 230 +-30 мм и внутреннего расстояния между подлокотниками в пределах 350 - 500 мм;

14. Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм;

15. Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.1.5. Требования к электробезопасности

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

Согласно документу «Правила устройства электроустановок (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;

2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.1.6. Рекомендации по организации режима труда и отдыха пользователя

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности согласно СанПиН 2.2.2/2.4.1340-03.

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы А категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

1. Категория – до 20 000 знаков;

2. Категория – до 40 000 знаков;

3. Категория – до 60 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать двух часов. При восьмичасовой рабочей смене и работе на ВДТ и ПЭВМ регламентированные перерывы следует устанавливать:

1. Для 1 категории работ через 2 ч. от начала рабочей смены и через 2 ч. после обеденного перерыва продолжительностью 15 мин. каждый;

2. Для 2 категории работ через 2 ч. от начала рабочей смены и через 1,5–2 ч. после обеденного перерыва продолжительностью 15 мин. каждый или продолжительностью 10 мин. через каждый час работы;

3. Для 3 категории работ через 2 ч. от начала рабочей смены и через 1,5−2,0 ч. после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин. через каждый час работы.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения

мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ВДТ и ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ВДТ и ПЭВМ.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций, инструкций и т.п. Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

4.2. Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) "О противопожарном режиме" устанавливают следующие правила:

1. В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее - руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями;

2. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

3. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

4. Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума;

5. Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности;

6. Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте;

7. В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны;

8. На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре;

9. На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте;

10. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации;

11. Запрещается на территориях, прилегающих к объектам, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных некоммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами;

12. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности;

13. Руководитель организации обеспечивает устранение повреждений толстослойных напыляемых составов, огнезащитных обмазок, штукатурки, облицов-

ки плитными, листовыми и другими огнезащитными материалами, в том числе на каркасе, комбинации этих материалов, в том числе с тонкослойными вспучивающимися покрытиями строительных конструкций, горючих отделочных и теплоизоляционных материалов, воздуховодов, металлических опор оборудования и эстакад, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией завода-изготовителя с составлением протокола проверки состояния огнезащитной обработки (пропитки). Проверка состояния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год;

14. Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями;

15. На объектах запрещается:

15.1. Хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности;

15.2. Использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов;

15.3. Размещать в лифтовых холлах кладовые, киоски, ларьки и другие подобные помещения;

15.4. Устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается

нормативными документами по пожарной безопасности, если нет самостоятельного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток;

15.5.Снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

15.6.Производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией);

15.7.Загромождать мебелью, оборудованием и другими предметами двери, люки на балконах и лоджиях, переходы в смежные секции и выходы на наружные эвакуационные лестницы, демонтировать межбалконные лестницы, заваривать и загромождать люки на балконах и лоджиях квартир;

15.8.Проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня;

15.9.Остеклять балконы, лоджии и галереи, ведущие к незадымляемым лестничным клеткам;

15.10. Устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы;

15.11. Устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла;

15.12. Устанавливать в лестничных клетках внешние блоки кондиционеров;

15.13. Загромождать и закрывать проходы к местам крепления спасательных устройств;

16. Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) зданий и сооружений в исправном состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие;

17. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов;

18. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

19. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

20. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

21. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

22. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

23. Запрещается:

23.1.эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

23.2.пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

23.3.обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

23.4.пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

23.5.применять нестандартные (самодельные) электронагревательные приборы;

23.6.оставлять без присмотра включенными в электрическую сеть электронагревательные приборы, а также другие бытовые электроприборы, в том числе находящиеся в режиме ожидания, за исключением электроприборов, которые могут и (или) должны находиться в круглосуточном режиме работы в соответствии с инструкцией завода-изготовителя;

23.7.размещать (складировать) в электрощитовых (у электрощитов), у электродвигателей и пусковой аппаратуры горючие (в том числе легковоспламеняющиеся) вещества и материалы;

23.8.при проведении аварийных и других строительно-монтажных и реставрационных работ использовать временную электропроводку, включая удлинители, сетевые фильтры, не предназначенные по своим характеристикам для питания применяемых электроприборов.

24. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы;

25. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы на расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра - по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами);

26. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре;

27. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

27.1.оставлять двери вентиляционных камер открытыми;

27.2.закрывать вытяжные каналы, отверстия и решетки;

27.3.подключать к воздуховодам газовые отопительные приборы

27.4.выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества;

28. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год;

29. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год);

30. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

31. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009 таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда, повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара.

Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя

периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

4.3. Микроклимат

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории 1а.

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах».

Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 2.

Таблица 2. Оптимальные величины параметров микроклимата для категории работ 1а (СанПиН 2.2.4.3359-16).

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	1а (до 139)	22–24	21–25	60–40	0,1
Теплый	1а (до 139)	23–25	22–26	60–40	0,1

В помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.

4.4. Вывод по четвертой главе

В данной главе дипломной работы были описаны общие требования к организации рабочих мест пользователей, требования к пожаро- и электробезопасности. Созданные условия должны обеспечивать комфортную работу. Соблюдение условий, описанных в данной главе, определяющих оптимальную организацию рабочего места, позволит сохранить хорошую работоспособность в течение всего рабочего дня, повысит как в количественном, так и в качественном отношениях производительность труда сотрудника организации.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы были изучены нормативно – правовые акты в сфере защиты информации. Была разработана информационно - аналитическая система, готовая к внедрению в различные организации.

В теоретической части выделена значимость информационно – аналитической деятельности в конфиденциальном документообороте. Результатом теоритической части является разработка инструкции по конфиденциальному делопроизводству.

Был проведён сравнительный обзор некоторых программных решений отечественных и зарубежных производителей. Для создания системы была выбрана ИСУБД CronosPro.

В практической части работы была разработана система. В рамках работы представлены некоторые части системы, структура и примеры информационно - аналитической системы представлены в приложениях.

Созданная в рамках работы информационно – аналитическая система, а также инструкция по конфиденциальному делопроизводству , позволяет практически в полной мере ввести режим коммерческой тайны на любом предприятии или организации.

ПРИЛОЖЕНИЕ А

УТВЕРЖДЕНО
Приказом
от «___» _____ 2017 г. № ___

ИНСТРУКЦИЯ
по конфиденциальному делопроизводству в ООО “ВЫМПЕЛ”

Настоящая “Инструкция по конфиденциальному делопроизводству в ООО “ВЫМПЕЛ”” (далее по тексту – Инструкция) разработана с целью защиты информации ограниченного доступа в ООО “ВЫМПЕЛ”, на основании Федеральных законов: от 27 июля 2006 года № 149-ФЗ “Об информации, информационных технологиях и защите информации”, от 27 июля 2006 года № 152-ФЗ “О персональных данных”, от 29 июля 2004 года № 98-ФЗ “О коммерческой тайне”.

1. Общие положения

1.1. Инструкция устанавливает общие требования, предъявляемые к регистрации, учёту, оформлению, тиражированию, хранению, использованию и уничтожению конфиденциальных документов независимо от вида носителя конфиденциальной информации. Выполнение требований Инструкции является обязательным для работников ООО “ВЫМПЕЛ”, получившим доступ к конфиденциальной информации и другим сведениям ограниченного доступа ООО “ВЫМПЕЛ” .

1.2. В ООО “ВЫМПЕЛ” ведение кконфиденциального делопроизводства возлагается на канцелярию, кроме того, руководитель предприятия назначает ответственных за ведение конфиденциального делопроизводства в отдельных структурных подразделениях.

Права и обязанности работников, ответственных за ведение конфиденциального делопроизводства в ООО “ВЫМПЕЛ”, закрепляются в их должностных инструкциях.

Должностные лица, допущенные к работе с конфиденциальной информацией и другими сведениями ограниченного доступа ООО “ВЫМПЕЛ”, несут персональную ответственность за правильный учёт, хранение, копирование и использование конфиденциальных документов в соответствии с требованиями настоящей Инструкции.

1.3. Контроль за организацией работы с конфиденциальными документами осуществляется канцелярией а в подразделении ответственными за ведение конфиденциального делопроизводства.

1.4. Отнесение информации к сведениям, составляющим коммерческую тайну, производится в соответствии с перечнем информации, составляющей коммерческую тайну, который регламентирован приказом предприятия № ___ от _____ г. “О защите конфиденциальной и иной охраняемой информации”.

1.5. Документы, содержащие сведения, составляющие коммерческую тайну, иную информацию конфиденциального характера (далее по тексту - конфиденциальные документы), являются собственностью предприятия, которое в полном объеме реализует в отношении них полномочия владения и распоряжения.

1.6. Ответственность за организацию и состояние конфиденциального делопроизводства, за обращение с конфиденциальными документами, своевременное, качественное их исполнение и оформление, в соответствии с внутренними нормативными требованиями по конфиденциальному делопроизводству и их сохранность в структурных подразделениях предприятия возлагается на руководителей структурных подразделений и выделенных сотрудников.

Они в свою очередь:

– организуют своевременную передачу конфиденциальных документов по назначению,

– организуют сохранность образующихся в текущем делопроизводстве конфиденциальных документов до сдачи их в архив предприятия или уничтожения,

– об утрате конфиденциальных документов в своём структурном подразделении незамедлительно докладывают директору по подчиненности или лицу его замещающему, или руководителю предприятия,

– несут личную ответственность в случае нарушения требований к организации конфиденциально делопроизводства.

Продолжение приложения А

1.7. Работники, назначенные ответственными за ведение конфиденциального делопроизводства в структурных подразделениях, обязаны:

−знать и строго выполнять требования настоящей инструкции и приказа предприятия №__ от ____ г. “О защите конфиденциальной и иной охраняемой информации в ООО “ВЫМПЕЛ” ”,

−знать основы конфиденциального делопроизводства, правила составления основных видов документов предприятия: заявлений, служебных записок, писем и т.д.,

−вести дела с конфиденциальными документами, хранящиеся в структурных подразделениях, в соответствии с утверждённой номенклатурой дел, своевременно готовить и передавать законченные дела в архив предприятия,

−нести ответственность за надлежащее исполнение требований настоящей Инструкции, сохранность находящихся у них конфиденциальных документов,

−об утрате конфиденциальных документов незамедлительно докладывать руководителю структурного подразделения.

1.8. Вновь принятые работники, которые, в соответствии с возложенными на них должностными обязанностями, связаны с конфиденциальным делопроизводством предприятия, должны быть ознакомлены под роспись с настоящей Инструкцией, установленным порядком работы и номенклатурой дел, содержащих конфиденциальные документы. Также пройти аттестацию на знание и понимание положений настоящей Инструкции.

1.9. При переходе на другую работу или увольнении работника, ответственного за ведение конфиденциального делопроизводства на предприятии или в структурных подразделениях, составляется совместно с работником, на которого возлагается исполнение этих функций, акт приема-передачи дел, печатей, штампов и журналов регистрации конфиденциальных документов.

Продолжение приложения А

1.10. Всю ответственность за сохранность конфиденциальных документов и неразглашение содержащихся в них сведений несут работники, осуществляющие работу с этими документами.

2. Термины и определения

Защита информации - деятельность, направленная на предотвращение разглашения защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Конфиденциальное делопроизводство - отрасль деятельности предприятия, обеспечивающая строгое соблюдение порядка приема, учета, подготовки, оформления, размножения (тиражирования), контроля исполнения, хранения, использования, отправки и уничтожения конфиденциальных документов на предприятии.

Носитель защищаемой 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.

Документированная информация (документ) - зафиксированная на материальном носителе защищаемая информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Информация (сведения) конфиденциального характера - коммерческая тайна, персональные данные, сведения, составляющие тайну следствия и судопроизводства, врачебная, нотариальная, адвокатская тайна, тайна переписки и другие сведения в соответствии с Указом Президента Российской Федерации от 6 марта 1997г. № 188 “Об утверждении перечня сведений конфиденциального характера”;

Продолжение приложения А

Информация, составляющая коммерческую тайну - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства - ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые предприятием меры по защите информации.

В тексте данной инструкции, при построении блок-схем, используются следующие сокращения, обозначения, символы:

ЗАО - закрытое акционерное общество;

О - ответственный;

И - исполнитель;

У - участник;

Рук - руководитель ЗАО или структурного подразделения;

СП - структурное подразделение;

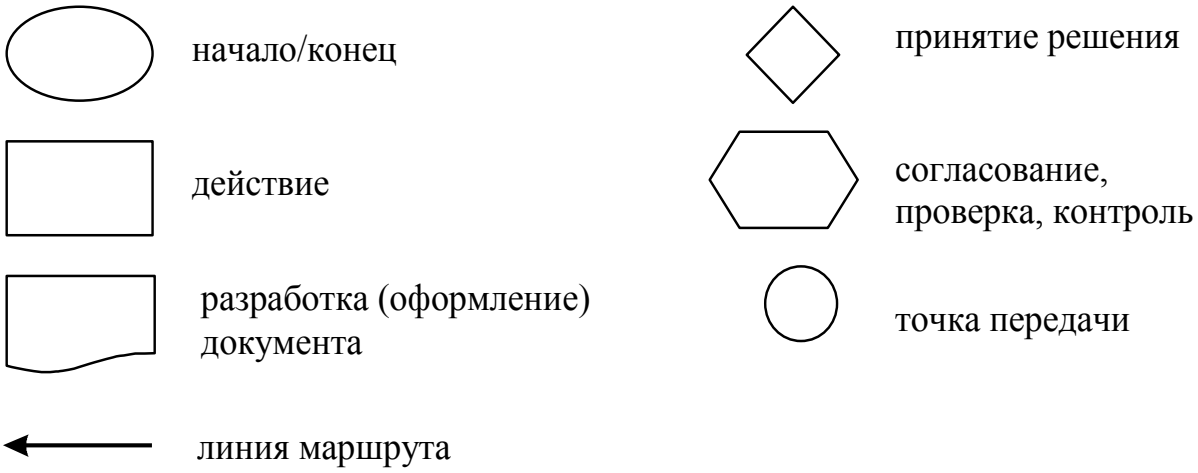
Канц - СП, обеспечивающее ведение делопроизводства, в т.ч. конфиденциального;

Сек - секретарь руководителя предприятия;

Сотр - сотрудник СП, непосредственно работающий с конфиденциальными документами;

Спец - специалист канцелярии или структурного подразделения, ответственный за ведение конфиденциального делопроизводства.

Продолжение приложения А



3. Конфиденциальные документы предприятия

3.1. Документирование управленческой деятельности предприятия заключается в записи по установленным правилам информации, требуемой для создания документа на материальный носитель, т.е. в создании документа. Виды конфиденциальных документов, издаваемых на предприятии:

−организационные документы (положения, инструкции);

−нормативные документы (стандарты, правила);

−распорядительные документы (приказ, распоряжение);

−информационно-справочные документы (акт, протокол, докладная записка, объяснительная записка, служебная записка, заявление, письмо, справка, доклад и др.).

3.2. На предприятии выделяется три группы конфиденциальных документов:

−внутренние - образуются в результате внутренней деятельности предприятия, не выходящие за его пределы, им присваивается буквенный индекс – “уч.”;

−входящие - поступающие на предприятие из сторонних организаций, им присваивается буквенный индекс “вх.”;

–исходящие - отправляемые в другие организации, им присваивается буквенный индекс “исх.”.

4. Порядок подготовки, оформления документов и учета материальных носителей конфиденциальной информации

4.1. Подготовка, оформление и согласование конфиденциальных документов осуществляются в соответствии с учётом требований настоящей Инструкции.

4.2. Конфиденциальная информация может содержаться на бумажных и электронных носителях.

4.3. На документы, содержащие конфиденциальную информацию, исполнителем документа, руководителем подразделения - исполнителя документа или должностным лицом, подписывающим (утверждающим) документ, в правом верхнем углу проставляются гриф конфиденциальности **“Конфиденциально”** - на документах, содержащих конфиденциальную информацию в соответствии с Перечнем конфиденциальной информации (далее - Перечень), также указывается номер пункта, согласно перечня к которому относится данный документ по форме согласно приложению № 1.

Соответствующий гриф конфиденциальности проставляется на электронных версиях документов, содержащих конфиденциальную информацию.

4.4. Бумажные и электронные конфиденциальные документы до подписания и присвоения исходящего регистрационного номера документу подлежат учёту в Журнале учета конфиденциальных документов (приложение № 2) работником, ответственным за ведение конфиденциального делопроизводства.

Учётный номер бумажного носителя конфиденциальной информации состоит из буквенного обозначения “К” (для конфиденциальной информации) и порядкового номера по Журналу учёта проектов документов на бумажных носителях, записываемых через косую черту (например, К-Б/4, К – признак

конфиденциальной информации, Б – бумажный носитель, 4 – порядковый номер носителя по Журналу).

4.5. Внешние электронные накопители (CD-диски, USB - накопители) и другие накопители, используемые для хранения конфиденциальной информации, подлежат учету в Журнале (приложение № 3). На электронных накопителях гриф “Конфиденциально” и учётный номер носителя информации указываются на бумажной наклейке. Указанные реквизиты должны быть нанесены также на CD-диски. Гриф конфиденциальности и учётный номер носителя наносятся специальным маркером.

Учётный номер электронного носителя конфиденциальной информации состоит из буквенного обозначения “К-Э” и порядкового номера по Журналу, которыы записываются через косую черту (например, К-Э/7, “К” – признак конфиденциальной информации, “Э” – внешний электронный накопитель, “7” – порядковый номер носителя по Журналу).

Применение личных носителей информации работников, в компьютерах содержащих документы для служебного пользования и конфиденциальную документацию, запрещается.

Запрещается записывать на внешние электронные накопители, не имеющие гриф “Конфиденциально”, файлы, содержащие конфиденциальную информацию.

4.6. Гриф без кавычек проставляется в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к конфиденциальным материалам.

На документе ниже грифа конфиденциальности указывается номер экземпляра, также указывается номер пункта, согласно перечня к которому относится данный документ, например:

Продолжение приложения А

Конфиденциально
Согласно п.перечня №
Экз. №

Адресат

На оборотной стороне последнего листа каждого экземпляра документа в левом нижнем углу указывается учётный номер документа по Журналу конфиденциальных документов (приложение № 2), количество отпечатанных экземпляров, количество листов в каждом экземпляре, фамилия исполнителя, его телефон и дата подготовки документа, например:

Уч. № … *(№ по Журналу учета проектов документов на бумажных носителях конфиденциальной информации)*
Отп. 2 экз., на 5 л. каждый
Экз. № 1 – в адрес
Экз. № 2 – в дело
И.И.Иванов
8-45
21.02.2017

Учётный номер носителя информации указывается также в левом нижнем углу лицевой стороны каждого листа документа (печатается шрифтом № 10).

4.7. Если к конфиденциальному документу прилагаются другие материалы (документы), то они перечисляются в конце текста письма в “Приложении” с указанием: краткого наименования, грифа “Конфиденциально”, номера документа, номера экземпляра, количества листов (по каждому приложению отдельно, в том числе и не конфиденциальному), например:

Продолжение приложения А

Приложение: 1. Сведения о..., конфиденциально, № ___, экз. № 1,
на 4 л.
2. Справка ..., на 3 л.

В тех случаях, когда приложение направляется без оставления копии в делах отправителя, после перечисления реквизитов приложения указывается: “только адресату”, а если адресатов несколько, указывается какому адресату, например: “Только в первый адрес”.

Гриф конфиденциальности необходимо проставлять и на сопроводительном письме к конфиденциальным материалам (документам).

Если в сопроводительном письме не содержится конфиденциальных сведений, то на нём под грифом конфиденциальности указывается: “Без приложения не конфиденциально”.

4.8. Разработанные проекты конфиденциальных документов представляются исполнителями руководителям на визирование или подпись, а также направляются для согласования по реестру (приложение № 4).

5. Работа с входящими, исходящими и внутренними конфиденциальными документами

5.1. Работа с входящими, исходящими и внутренними конфиденциальными документами организуется в соответствии с учётом требований настоящей Инструкции. Каждая из перечисленных групп документов имеет свои особенности обработки, регистрации и хранения

5.2. Обработка и регистрация входящих документов:

5.2.1. Работа с входящими документами начинается с получения корреспонденции в отделении почтовой связи, доставки документов курьерскими службами, посредством электронной почты или факса.

Продолжение приложения А

5.2.2. Прием и сортировка входящей корреспонденции осуществляется централизовано Спец Канц.

5.2.3. Поступающие документы с грифом конфиденциальности вскрываются (кроме указанных далее в пунктах), с проверкой правильности адресации и целостности упаковки документов.

5.2.4. Конверты (пакеты) с грифом “Конфиденциально”, содержащие дополнительную отметку ***“Лично”***, не вскрываются, регистрируются как документы и передаются непосредственно адресату под роспись в Журнале регистрации входящих конфиденциальных документов. Конверты (пакеты) вскрываются ***лично адресатом***, на первый лист документа переносится номер и дата регистрации конверта (пакета). Записи о ходе исполнения таких документов осуществляются по письменному поручению адресата Спец Канц или СП.

5.2.5. Предварительное рассмотрение документов проводится с целью распределения поступившей корреспонденции по СП.

5.2.6. Документы регистрируются Спец Канц в день их поступления в журналах (приложение № 5).

5.2.7. В правом нижнем углу документа проставляется штамп с наименованием предприятия, указанием даты поступления и входящим регистрационным номером.

5.2.8. Зарегистрированная конфиденциальная корреспонденция передается Спец Канц в СП, с обязательной отметкой (подписью) в Реестре передачи конфиденциальных документов (Приложение № 4).

5.2.9. Документы, полученные из правительственных и вышестоящих органов управления РФ, адресованные Рук ЗАО, передаются Спец Канц Сек.

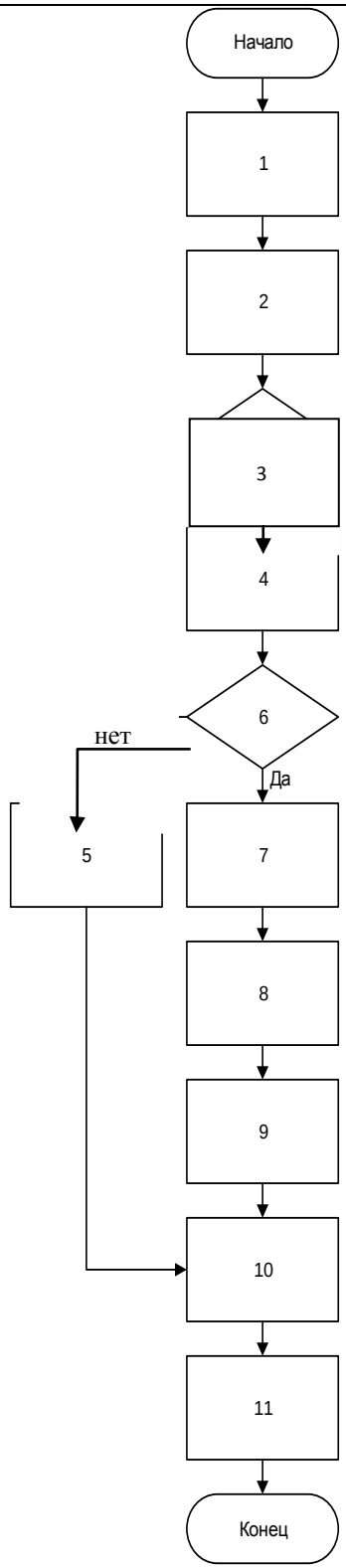
5.2.10. Рассмотренные Рук ЗАО документы возвращаются Сек, который вносит содержание резолюции в журнал регистрации, после чего документ передается на исполнение. Документы, исполняемые несколькими СП, передаются им поочередно или одновременно в копиях. Подлинник передается Рук СП, названному в резолюции первым.

5.2.11. Спец СП периодически получают корреспонденцию в Канц. Срочная корреспонденция должна быть получена немедленно, по звонку Спец Канц.

5.2.12. С момента получения до передачи на исполнение, хранение или уничтожение, документы хранятся в СП. Сохранность документов обеспечивают Рук, Спец или Сотр СП согласно распределению ответственности, закрепленному в номенклатуре дел подразделения. В случае утраты какого-либо дела или документа, Сотр СП обязан незамедлительно известить об этом Рук СП.

5.2.13. Алгоритмы управления приведены в таблице 1.

Таблица 1



Действия	О	И	У
1 Получение входящей корреспонденции (5.2.1)	Рук Кацн	Спец Канц	
2. Сортировка входящей корреспонденции, первичная обработка (5.2.2- 5.2.4)	Рук Канц	Спец Канц	
3 Принятие решения о регистрации документов (5.2.5)	Рук Канц	Спец Канц	
4 Регистрация входящей корреспонденции, включая электронные документы (5.2.6; 5.2.7)	Рук Канц	Спец Канц	
5 Передача корреспонденции в СП (в том числе нерегистрируемой и срочной) (5.2.8)	Рук Канц	Спец Канц	Спец СП
6 Принятие решения о рассмотрении документов Рук ЗАО (5.2.9)	Рук Канц	Рук Канц	Спец Канц
7 Рассмотрение документов Рук ЗАО	Рук ЗАО	Рук ЗАО	Сек
8 Внесение сведений резолюции в журналы регистрации документов (5.2.10)	Рук ЗАО	Сек	Спец Канц
9 Передача документов на исполнение (5.2.10)	Рук Канц	Сек Спец Канц	
10 Получение корреспонденции в Канц (5.2.11)	Рук СП Рук Канц	Спец Канц Спец СП	Сотр СП
11 Хранение документов в СП (5.2.12)	Рук СП	Сотр СП	Спец СП

5.3. Обработка и регистрация исходящих документов.

5.3.1. Под исходящими документами понимаются письма, подготовленные на бланках установленного образца.

5.3.2. Работа над исходящим документом состоит из составления проекта документа, согласования, подписания (утверждения), регистрации и отправки.

5.3.3. Проект исходящего документа составляется Сотр СП, в соответствии с требованиями ГОСТ Р 6.30 к подготовке писем.

5.3.4. Рук СП проверяет правильность оформления документа, наличие необходимых реквизитов и приложений. К проекту прикладываются материалы, на основании которых документ был подготовлен.

5.3.5. В ряде случаев проект исходящего письма должен быть согласован с другими СП ЗАО. Такое согласование оформляется визой Рук СП.

5.3.6. Рук СП подписывают исходящие документы в пределах предоставленных им прав, предусмотренных Положением о соответствующем подразделении, должностными инструкциями.

5.3.7. Регистрация исходящих документов осуществляется децентрализовано в журналах регистрации Канц (Приложение № 6): документы, подготовленные в СП, регистрируются Сотр СП, а документы, подготовленные Рук ЗАО регистрируются Спец Канц.

5.3.8. На документе проставляется регистрационный гриф “Конфиденциально”, номер и дата.

5.3.9. Копии исходящих документов подшиваются Спец СП, Спец Канц в дела с исходящей перепиской и хранятся в подразделении. Ответственность за формирование и сохранность дел в СП возлагается на их руководителей.

5.3.10. Документы, предназначенные для отправки средствами почтовой связи, доставляются Спец СП в Канц полностью оформленными, подписанными, зарегистрированными, вложенными в конверт с отметкой о категории почтового отправления (кроме простых отправлений) в канцелярию для дальнейшей обработки и отправки писем.

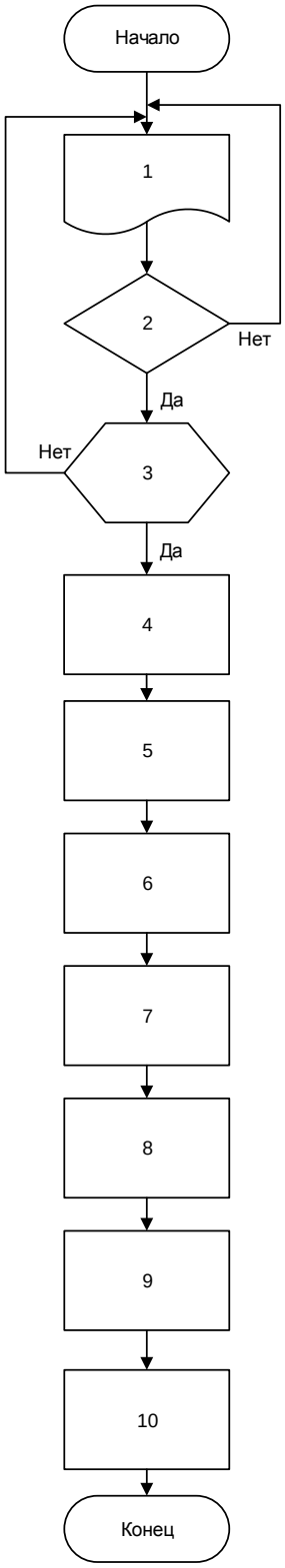
5.3.11. Необходимость отправки документов заказной почтой определяется исполнителем. В случае доставки адресатам пакетов с конфиденциальными документами курьерами (нарочными) документы им выдают под роспись в Журнале выдачи конвертов (пакетов) с грифом конфиденциальности (Приложение № 10). Доставка конфиденциальных конвертов (пакетов) осуществляется на служебном транспорте. Конверты (пакеты) передаются адресатам по реестру (Приложение № 11), в котором, кроме подписи о получении пакетов, проставляется печать получателя.
При направлении конфиденциальных документов в несколько адресов составляется список рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов (приложение № 14). Список рассылки подписывается исполнителем и утверждается руководителем подразделения - исполнителя документа.

5.3.12. Исполнитель несет ответственность за правильность адресования и наличие вложений почтового отправления.

5.3.13. Подготовленные к отправке конверты с документами, Спец Канц, маркируются, на все почтовые отправления составляются реестры, на заказные отправления в двух экземплярах, один из которых остается в отделении связи. Вся отправляемая корреспонденция доставляется Спец Канц в отделение почтовой связи.

5.3.14. Алгоритмы управления приведены в таблице в таблице 2.

Таблица 2



Действие	О	И	У
1 Составление проекта документа исполнителем (5.3.3)	Рук СП	Сотр СП	Соисполнители в СП
2 Проверка правильности оформления проекта документа (5.3.4)	Рук СП	Рук СП	
3 Согласование проекта документа (5.3.5)	Рук СП	Сотр СП	Рук других СП
4 Подписание документа руководителем	Рук ЗАО	Рук ЗАО	Сек
5 Регистрация исходящих документов: - в Канц (5.3.7)	Рук СП Рук Канц	Спец СП Спец Канц	Сотр СП
6 Подшивка копий исходящих документов в дела: в СП в Канц (5.3.9)	Рук СП Рук Канц	Спец СП Спец Канц	Сотр СП
7 Подготовка документов (к отправке, включая их упаковку в конверты и заполнение конвертов) в СП (5.3.10)	Рук СП	Спец СП Сотр СП	Спец Канц
8 Передача исходящих документов в Канц для отправки (5.3.10)	Рук СП	Спец СП	Спец Канц
9 Взвешивание, маркировка, составление реестров на отправку документов (5.3.13)	Рук Канц	Спец Канц	
10 Передача исходящих документов в отделение почтовой связи для последующей отправки (5.3.13)	Рук Канц	Спец Канц	

5.4. Работа с внутренними конфиденциальными документами.

5.4.1. Проекты документов готовятся исполнителем, затем передаются на согласование и подписание (утверждение).

5.4.2. Подписанные (утвержденные) руководством подлинники документа со всеми приложениями и, при необходимости, электронные копии предоставляются исполнителями в Канц для регистрации и рассылки в СП, в ведении которых находятся рассматриваемые вопросы.

5.4.3. Подлинники конфиденциальных документов регистрируются Канц в Журнале документов конфиденциальной информации (Приложение № 2). В электронной копии указывается регистрационный номер и дата регистрации документа. Канц проверяет соответствие электронной копии документа оригиналу.

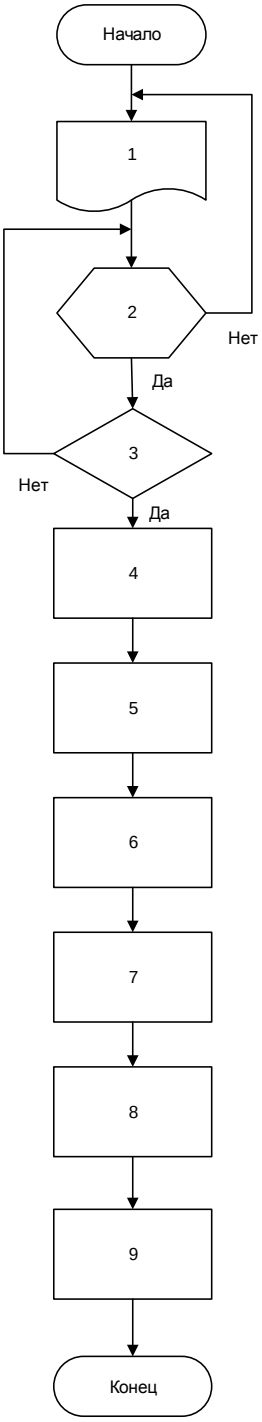
5.4.4. Передача зарегистрированной документации в СП производится Канц по реестру.

5.4.5. Приобщение подлинников документов в дела осуществляется Канц или СП.

5.4.6. Завершающими стадиями работы с внутренними конфиденциальными документами являются: использование в справочно-информационной работе и определение сроков хранения.

5.4.7. Алгоритм и матрица распределения ответственности приведены в таблице 3.

Таблица 3



Действие	О	И	У
1 Составление (5.4.1)	Рук СП	Сотр СП	другие Сотр СП
2 Согласование (5.4.1)	Рук СП	Сотр СП	другие Сотр СП
3 Утверждение документа (5.4.1)	Рук ЗАО	Рук СП	Сек
4 Передача утвержденных документов в Канц (5.4.2)	Рук СП	Спец СП	
5 Регистрация документа (5.4.3)	Рук Канц	Спец Канц	Спец Канц
6 Рассылка копий документа в структурные подразделения (в бумажном/электронном виде) (5.4.4)	Рук Канц	Спец Канц	Спец СП
7 Приобщение документов в дела Канц (5.4.5)	Рук Канц	Спец Канц	
8 Приобщение документов в дела СП (5.4.5)	Рук СП	Спец СП	
9 Использование документа в справочно-информационной работе (5.4.6)	Рук СП Рук Канц	Спец СП Спец Канц	Сотр СП

6. Номенклатура дел

6.1. Номенклатура дел составляется и утверждается совместно с РУК СП и РУК Канц.

6.2. Далее, СОТР СП получают обложки дел в Канц с записью в журнале (приложение № 15).

6.3. Входящие и внутренние документы, которые находятся в исполнении у СОТР СП в течении некоторого времени должны быть обязательно приобщены в дела.

6.4. Для приобщения в дело СОТР СП должен в Канц проставить отметку о приобщении документа в дело(приложение № 2, значение ”Приобщен в дело”).

7. Приобщение конфиденциальных документов в дела

7.1. Каждому номенклатурному делу, в которое приобщаются конфиденциальные документы присваивается гриф конфиденциальности. В номенклатуре дел в графе “Номер дела” к номеру дела добавляется отметка “К”.

7.2. В номенклатуры дел в обязательном порядке включаются и журналы учёта конфиденциальных документов.

7.3. После исполнения документы подшиваются в дело. Конфиденциальные документы не могут быть подшиты в дела без грифа “Конфиденциально”.

7.4. Дата начала дела должна соответствовать дате первого подшитого в дело конфиденциального документа, дата окончания дела - дате последнего конфиденциального документа, подшитого в нём. Эта дата проставляется на обложке дела после того, как в него будет подшит последний документ.

7.5. Все подшитые в дело (том) конфиденциальные документы нумеруются полистно, номера проставляются простым карандашом в правом верхнем углу листа документа. На подшитые конфиденциальные документы составляется внутренняя опись (приложение № 7), которая заполняется по мере подшивки в дело документов.

Листы внутренней описи дела нумеруются отдельно. Листы ознакомления с распорядительными конфиденциальными документами (приложение № 7, примечание) подшиваются в дела вместе с этими документами, вносятся во внутреннюю опись и нумеруются.

По окончании дела (тома) в конце внутренней описи указывается (цифрами и прописью) количество внесенных в неё документов, а также должность и фамилия работника, ответственного за ведение конфиденциального делопроизводства.

7.6. Законченное дело (том) с документами прошивается, опечатывается и заверяется работником, ответственным за ведение конфиденциального делопроизводства. Опечатывание дела (тома) производится с помощью бумажной наклейки с оттиском печати “Для пакетов”, которая наклеивается так, чтобы захватывались нити шнурка прошивки дела (тома).

7.7. Во внутренней описи переходящего дела после ежегодной проверки наличия документов комиссией делается итоговая запись о количестве подшитых в деле листов по состоянию на 31 декабря каждого года, которая заверяется подписью председателя экспертной комиссии. Нумерация листов дела после итоговой записи продолжается от номера последнего листа прошлого года.

7.8. По окончании календарного года дело с грифом “Конфиденциально” просматривается полистно экспертной комиссией и, в случае необходимости, принимается решение о перегруппировке документов. Содержащиеся в этом деле документы, постоянное хранение которых вызывается служебной необходимостью, группируются в отдельное дело (дела), которое получает самостоятельный заголовок и дополнительно включается в номенклатуру дел.

Если в дело включены документы только временных сроков хранения, оно может не переформировываться. Срок хранения такого дела устанавливается по максимальному сроку хранения содержащихся в нём документов.

7.9. Приём дел с грифом конфиденциальности на постоянное хранение оформляется актом приема-передачи (приложение № 8). Дела передаются с обязательной полистной проверкой включенных в них документов.

7.10. Дела с грифом конфиденциальности постоянного хранения выдаются только тем исполнителям, которые имеют к ним прямое отношение для исполнения своих служебных обязанностей, на основании письменного запроса Рук СП. Выдача дел осуществляется под расписку в карточке учёта выдачи дел (Приложение № 9).

7.11. Ответственность за приём, хранение и выдачу дел с грифом конфиденциальности постоянного хранения возлагается на Рук Канц.

8. Хранение конфиденциальных документов

8.1. С момента заведения и до передачи в архив Канц дела хранятся по месту их формирования. В этот период ответственность за сохранность конфиденциальных документов и содержащейся в них защищаемой информации несут Рук СП.

8.2. Документы, дела и другие конфиденциальные материалы должны храниться в сейфах, запираемых шкафах (ящиках). К хранению документов предъявляются следующие требования:

– помещение для хранения конфиденциальной информации должно быть оборудовано специальными шкафами или сейфами, запирающимися и опечатывающимися;

– хранение открытых документов вместе с конфиденциальными допускается только в тех случаях, когда они являются приложениями к конфиденциальным документам;

– получение конфиденциальной информации из архива возможно только с письменного разрешения Рук Канц или Рук ЗАО.

8.3. За сохранность конкретного конфиденциального документа отвечает работник, получивший этот документ в пользование под расписку.

8.4. Передача конфиденциальных документов от одного работника другому производится с обязательной отметкой в журнале (приложение № 4).

8.5. При замене или увольнении работника, ответственного за ведение конфиденциального делопроизводства, составляется акт приема-передачи конфиденциальных документов, утверждаемый руководителем подразделения (приложение № 8).

8.6. Запрещается выносить документы, дела и другие конфиденциальные материалы из служебных помещений для работы с ними на дому, в гостинице и т.д.

В необходимых случаях Рук ЗАО может в письменной форме разрешить исполнителям или другим работникам вынос из здания конфиденциальных документов для их согласования, подписи и т.п.

8.7. Командируемым работникам под их личную ответственность, с письменного разрешения Рук ЗАО разрешается иметь при себе в пути следования конфиденциальные материалы.

8.8. О фактах утраты конфиденциальных документов, дел и других материалов либо разглашения содержащихся в них сведений немедленно ставятся в известность Рук ЗАО.

8.9. По факту утраты конфиденциальных документов, дел и других материалов или разглашения сведений, содержащихся в этих материалах, проводится служебное расследование и составляется акт, который представляется Рук ЗАО для принятия решения.

9. Тиражирование конфиденциальных документов

9.1. Тиражирование документов, содержащих конфиденциальную информацию, большого объёма или требующих снятия значительного числа копий, производится на основании письменной заявки Рук СП, в интересах которого будет производиться тиражирование, с письменного разрешения (указания) Рук ЗАО.

В заявке указывается полное наименование документа, гриф конфиденциальности, количество листов и тираж.

9.2. Заявка, с письменным разрешением (указанием) Рук ЗАО и документы, предназначенные для тиражирования, представляются Спец Канц (передача осуществляется по реестру – приложение № 4).

9.3. Работы по тиражированию конфиденциальных материалов, а также уничтожению пробных и бракованных копий документов проводятся в присутствии Спец Канц. Тиражирование документа производится только на специально отведенном для этого копировальном аппарате.

9.4. Предназначенные для размножения документов технические средств должны быть защищены от несанкционированного доступа.

9.5. Размножение конфиденциальных документов не должно производиться вперемежку с размножением открытых документов. Во время размножения конфиденциальных документов все, что не имеет отношения к их размножению, должно быть убрано с рабочих мест, используемых при размножении, доступ посторонних лиц в помещение, в котором производится размножение, не разрешается.

9.6. В случае выполнения работ с использованием съемных электронных носителей, электронные копии конфиденциальных материалов в компьютере уничтожаются.

9.7. После размножения документов в Журналы регистрации конфиденциальных документов вносится соответствующая отметка о количестве полученных копий “Количество экземпляров.”, в соответствующей графе (приложение № 2). Дополнительно размноженные документы учитываются за номером основного документа. При этом запись о дополнительно отпечатанных экземплярах производится отдельной строкой. Порядковый номер полученной копии проставляется через косую черту, например: экз.№ 3/1, где “3” – экземпляр размножаемого документа, а “1” – порядковый номер размноженной копии.

9.8. На оборотной стороне документа проставляется штамп “Дополнительно размножено ___ экз.” с указанием номеров полученных копий.

10.Уничтожение конфиденциальных документов

10.1. Уничтожение материалов, содержащих конфиденциальную информацию, производится Комиссией по вопросам обеспечения защиты информации, создаваемую по приказу Рук ЗАО (далее по тексту – Комиссия)., на основании докладной записки Рук СП. В докладной записке указывается обоснование уничтожения конфиденциальных документов.

10.2. В состав Комиссии следует включать высококвалифицированных сотрудников, в первую очередь Рук и Спец Канц, а также Спец СП.

Председателем Комиссии назначается один из заместителей Рук ЗАО, допущенный ко всем конфиденциальным документам

10.3. Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста.

10.4. Конфиденциальная информация, хранящаяся на магнитных и/или электронных носителях, подлежит обязательному удалению путём полного форматирования носителя.

В целях гарантированного уничтожения файлов и затирания остаточной информации на магнитном носителе либо уничтожения носителей механическим способом Комиссия может привлечь специалистов по защите, чтобы зафиксировать факт уничтожения.

10.5. Факт уничтожения конфиденциальных материалов оформляется Комиссией соответствующим актом, утверждаемым Рук ЗАО (Приложение № 13).

10.6. После уничтожения материалов в журналах регистрации конфиденциальных документов и изданий, в номенклатурах и описях дел, а также в журналах учёта внешних электронных и других накопителей конфиденциальной

информации проставляется отметка “Уничтожено. Акт № __ от ___ (дата)”. Акты об уничтожении подшиваются в дела.

10.7. Подготовка предложений о снятии грифа конфиденциальности с документа по истечении указанного в Перечне срока действия режима ограничения доступа в отношении информации, содержащейся в документе, или в связи с исключением информации из Перечня возлагается на Комиссию. Заключение Комиссии оформляется составляемым в произвольной форме актом, утверждаемым председателем Комиссии. При этом на документе делается письменная отметка о снятии грифа “Гриф снят. Акт № ___ от _____ (дата)”, заверенная подписью лица, ответственного за ведение конфиденциального делопроизводства и печатью “Для пакетов”. Аналогичные отметки вносятся в описи дел.

11.Контроль за состоянием конфиденциального делопроизводства

11.1. По окончании календарного года Комиссией проводятся внутренние проверки наличия конфиденциальных документов.

11.2. Комиссия проверяет выполнение требований настоящей Инструкции, наличие текущих дел и дел с временными сроками хранения, наличие конфиденциальных документов, не подшитых в дела. Проверка наличия документов производится путём сверки журналов учёта с фактическим наличием документов, а также отметок об уничтожении или отправке документов в этих журналах с актами и реестрами.

11.3. В журналах учёта, переходящих из года в год, все произведённые отметки об отправке, уничтожении и переучёте конфиденциальных документов заверяются проставлением записи “Проверено” с датой и подписью председателя Комиссии.

11.4. К началу работы Комиссии все исполненные конфиденциальные документы должны быть учтены в конфиденциальном делопроизводстве, приобщены к делам.

11.5. По результатам работы Комиссии составляется акт проверки (Приложение № 14), который утверждается Рук ЗАО. В акте указываются результаты проверки конфиденциального делопроизводства, отмеченные недостатки и предложения по улучшению состояния дел по вопросам защиты конфиденциальной информации.

12. Учёт лиц, получивших доступ к конфиденциальной информации, и лиц, которым такая информация была предоставлена или передана

12.1. В Канц ведётся учёт:

–Сотр СП, получивших доступ к конфиденциальной информации и другим сведениям ограниченного доступа (далее – конфиденциальная информация), а также его контрагентов, и информации, к которой они получили доступ;

–должностных лиц органов государственной власти, иных государственных органов и органов местного самоуправления, получивших доступ к находящейся в ведении структурного подразделения конфиденциальной информации, в период проведения ими проверок либо иных мероприятий, проводимых в рамках полномочий данных органов власти, а также информации, к которой они получили доступ;

–органов государственной власти, иных государственных органов и органов местного самоуправления, которым была предоставлена в соответствии с их мотивированными требованиями (запросами) находящаяся в ведении структурного подразделения конфиденциальная информация, и переданных им материалов;

–контрагентов, которым в соответствии с заключёнными Соглашениями о конфиденциальности была передана конфиденциальная информация, и переданных им материалов, а также представителей контрагентов, получивших доступ к такой информации при выполнении работ.

12.2. Контроль за соблюдением порядка учёта лиц вышеуказанных

категорий осуществляет Рук Канц, а сам учёт осуществляет Спец Канц.

12.3. О лицах, получивших доступ к конфиденциальной информации, и лицах, которым такая информация была предоставлена или передана, Рук СП ежеквартально уведомляют Рук Канц.

13.Ответственность за неисполнение (ненадлежащее исполнение) настоящей Инструкции

13.1. Ответственность за соблюдение требований, установленных настоящей Инструкцией, несет Рук Канц, а также Рук и Сотр СП, допущенные к работе с конфиденциальными документами в соответствии с настоящей Инструкцией.

Продолжение приложения А
Приложение № 1

МУ

адрес тел. :

«____»_____200__г. №_____

на _____от «____»_____200__г

Конфиденциально
Согласно п.перечня №

Экз. №

Адресат

Краткое содержание документа

Т е к с т

Приложение: План …, конфиденциально, № …, экз. № 1, на 12 л.

(если приложение не остается у исполнителя, после количества листов указываются слова «только адресату»).

директор

_____ _____ _____
(личная подпись) (инициалы, фамилия)

Уч. № …
(№ по Журналу учета проектов документов на бумажных носителях конфиденциальной информации)

Образец

Продолжение приложения А

(оборотная сторона)

Образец

Уч. № … *(№ по Журналу учета проектов документов на бумажных носителях конфиденциальной информации)*

Отп. 2 экз., на 5 л. каждый

Экз. № 1 – в адрес

Экз. № 2 – в дело

И.И.Иванов

8-45

21.02.2017

Продолжение приложения А
Приложение № 2

Журнал учета конфиденциальных документов

Учётный номер документа	Дата регистрации	Пункт согласно перечню	Наименование	Количество листов	Кол-во экземпляров	Исполнитель	Примечание	Приобщен к делу
1	2	3	4	5	6	7	8	9

Продолжение приложения А
Приложение № 3

Журнал учёта внешних электронных и других накопителей,
используемых для хранения конфиденциальной информации

№№ п/п	Уч. №	Тип носи-теля	Объем па-мяти, МБ	Испол-нитель	Дата воз-врата	Отметка об уничто-жении (№ акта)
1	2	3	4	5	6	7

Приложение № 4

Реестр передачи конфиденциальных документов
между сотрудниками подразделения
(для доклада руководству подразделения,
выполнения работ по тиражированию)

№№ п/п	Учётный номер докумен-та	Наименова-ние докумен-та	Количест-во листов	Кому выдан(подраз-деление	Когда выдан
1	2	3	4	5	6

Продолжение приложения А
Приложение № 5

Журнал регистрации входящих конфиденциальных документов

№№ п/п	Входящий номер	Дата поступления	Адрес отправителя	Наименование документа		
					Количество листов документа	Количество листов приложения
1	2	3	4	5	6	7

Направлен на исполнение	Роспись
8	9

Продолжение приложения А
Приложение № 6

Журнал регистрации исходящих конфиденциальных документов

№№ п/п	Регистрационный номер документа	Адресат	Вид (способ) доставки адресату	Количество листов		Исполнитель	Примечание
				документа	приложения		
1	2	4	5	6	7	8	9

Продолжение приложения А
Приложение № 7

ВНУТРЕННЯЯ ОПИСЬ

документов, находящихся в деле № _____

том № _____ за 200__ год

Итого _____ документов.

(заполняется по окончании дела цифрами и прописью)

Количество листов внутренней описи _____ .

(цифрами и прописью)

Наименование должности лица, составившего внутреннюю опись документов дела — Подпись — И.О. Фамилия

«_____»_____200__ г.

Примечание: Во внутреннюю опись вносятся и нумеруются листы для ознакомления с распорядительными конфиденциальными документами, которые подшиваются в дела вместе с этими документами.

Продолжение приложения А
Приложение № 8

УТВЕРЖДАЮ

_____

(должность руководителя подразделения)

_____

(подпись) (И.О. Фамилия)

«____»_____ 200___г.

Акт приема-передачи документов (дел) с грифом «Конфиденциально»

_____

(наименование причины передачи документов)

№ № п/п	Номер и дата документа (индекс и крайние даты дела)	Заголовок документа (дела)	Количество листов документа (дела)
1	2	3	4

Всего _____ документов (дел)

(количество документов цифрами и прописью)

Передал _____ (должность, фамилия, имя, отчество)

Принял _____ (должность, фамилия, имя, отчество)

«___» _____ 200__ г.

Приложение № 9

Журнал учета выдачи дел с грифом «Конфиденциально»

Дата выдачи	Заголовок дела	Номер дела	Кому вручено	Дата возврата
1	2	3	4	6

Приложение № 10

Журнал выдачи курьерами конвертов (пакетов)
с грифом «Конфиденциально»

№№ п/п	Дата выдачи	Номер, указанный на конверте (пакете)	Адресат	Ф.И.О. курьера (нарочного)	Расписка в получении
1	2	3	4	5	6

Продолжение приложения А
Приложение № 11

Реестр передачи конвертов (пакетов)
с грифом «Конфиденциально»

Отправитель: _____
(отправитель и адрес)

№ № п/п	Адресат	№, указанный на конверте (пакете)
1	2	3

Всего _____ пакетов
(количество пакетов цифрами и прописью)

Подпись отправителя _____ (должность, фамилия, имя, отчество)

По настоящему реестру принято _____ пакетов

Подпись получателя _____ (должность, фамилия, имя, отчество)

Печать получателя

Продолжение приложения А
Приложение № 12

УТВЕРЖДАЮ
Наименование должности
руководителя

Подпись Расшифровка подписи

Дата

Список организаций
для рассылки документов с грифом «Конфиденциально»

_____ от «___» _____ 200__ г. № _____
(вид документа) (регистрационный номер документа)

№№ п/п	Наименование организации	Ф.И.О.	№ экз.	Расписка в получении документа	Расписка в сдаче документа
1	2	3	4	5	6

Исполнитель рассылки:

_____
(наименование подразделения _____)

_____ _____ _____ _____
(должность) (Ф.И.О.) (подпись) (телефон)

Дата рассылки: «___» _____ 200__ г.

Продолжение приложения А
Приложение № 13

Исполнительный Директор
_____

«_____»_____20___г.

А К Т
_____ № _____
_____
(место составления)
о выделении к уничтожению документов и дел с грифом «Конфиденциально», не подлежащих хранению

На основании _____

отобраны к уничтожению как утратившие практическое значение следующие дела и документы:

№ п/п	Заголовок дела или документа	Индекс дела по номенклатуре (или номер документа)	Срок хранения	Примечание
1	2	2	3	4

Документы уничтожены путем _____.

Председатель комиссии подпись должность, фамилия, инициалы

Члены комиссии: подписи должности, фамилии, инициалы

Продолжение приложения А

Приложение № 14

УТВЕРЖДАЮ

Исполнительный Директор _____

«_____»_____20___г.

А К Т

_____ № _____

_____

(место составления)

проверки наличия и состояния документов и дел с грифом «Конфиденциально» в

_____

(подразделение, в котором проводится проверка)

Основание _____

(плановая проверка, перемещение документов, стихийное бедствие и т.д.)

Проверкой, проведённой «___»_____200__г. Комиссией _____ _____в составе _____ установлено:

(т е к с т)

I. Всего числится по описям (номенклатурам дел, журналам учета) _____ (документов, дел)

(цифрами и прописью)

1) из них имеется в наличии _____
2) не обнаружено _____

(индексы (номера) документов, дел, изданий)

II. Обнаружено не внесенных в описи (номенклатуры дел, журналы учета) _____

III. Характеристика состояния документов, дел и изданий

_____

_____

Решение по результатам проверки:_____

_____

Председатель комиссии подпись должность, фамилия, инициалы

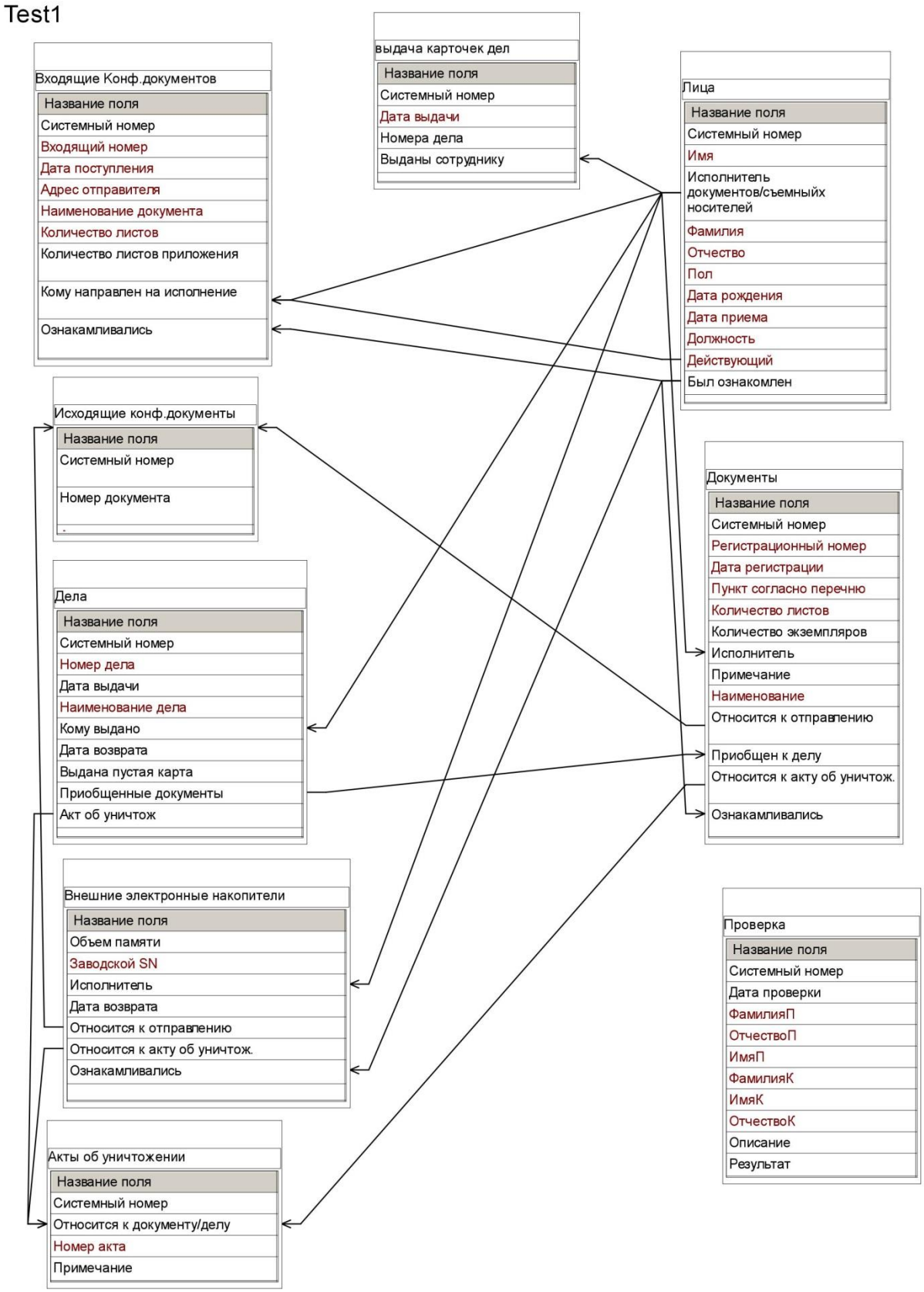
Члены комиссии: подписи должности, фамилии, инициалы

Приложение № 15

Журнал учета выдачи карточек дел

№№ п/п	Дата выдачи	Номер дела	Ф.И.О сотрудника	Расписка в получении
1	2	3	4	5

ПРИЛОЖЕНИЕ Б



БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149.
2. Шеннон К. Работы по теории информации. М., 1963.
3. Винер Н. Кибернетика и общество. М., 1958.
4. American National Standard Dictionary of Information Technology (ANSD).
5. Фомин Ю. А. Реальность невероятного. М.: Интербук, ТПО Старт, 1990
6. Юзвишин И. И. Основы информациологии. М.: Комкнига, 2000
7. Философский словарь/Под ред. И.Т. Фролова. Изд. 4-е. М.: Изд-во политической литературы, 1981.
8. Конопатов С.Н., Пинигин В.В. Информационно-аналитическая деятельность в современном управлении // Телекоммуникации и информатизация образования – 2006 - №6. - с. 11
9. Кулицкий С.П Основы организации информационной деятельности в сфере управления: навчпосибник /СП Кулицкий - К: МАУП 2002 – 224с.
10. Конотопов П.Ю Аналитика Методология, технологические и организационные аспекты информационно-аналитической работы / ПЮ Конотопов ЮВ Курносов - М: Русаки 2004 -250 с
11. Корнеев ИК Защита информации в офисе: учебник / ПК Корнеев ЕА Степанов - М: Велби 2007 - 336 с
12. Кузнецов И.М. Информация: поиск, анализ, защита: Учебник по информационно-аналитической работе. – М.: Яуза, 2001. – 320 с.
13. Захаров И.В., Филипов Л.Я. Основы информационно - аналитической деятельности.