

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине «Методы и средства защиты информации
в системах электронного документооборота»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026

ВВЕДЕНИЕ	3
ПРАКТИЧЕКАЯ РАБОТА № 1-3.....	5
ПРАКТИЧЕКАЯ РАБОТА № 4-6.....	10
ПРАКТИЧЕСКАЯ РАБОТА № 7-9.....	15

ВВЕДЕНИЕ

1. Цели и задачи освоения дисциплины:

Целью изучения дисциплины «Методы и средства защиты информации в системах электронного документооборота» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 Информационная безопасность.

Задачи освоения дисциплины «Методы и средства защиты информации в системах электронного документооборота»:

- ознакомление с методологическими принципами организации научного исследования;
- формирование системы базовых знаний об этапах научного исследования;
- уяснение предметной специфики эмпирического исследования;
- овладение современными методами сбора, хранения и обработки эмпирических данных, формирование представлений о современных технических средствах измерений и диагностики.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ИД-2 ОПК-3 разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности	оперирует основными нормативными правовыми актами в области обеспечения информационной безопасности; нормативными методическими документами ФСБ России в области защиты информации разрабатывает проекты
---	--	---

		нормативных материалов, регламентирующих работу по защите информации, нормативно-методические материалы по регламентации системы организационной защиты информации, организационно-распорядительную документацию по обеспечению информационной безопасности;
	ИД-3 ОПК-3 проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	Выделяет правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации анализирует экономическую информацию, возникающую в процессе производственно-хозяйственной деятельности, и вырабатывает рекомендации по экономической целесообразности ее защиты, анализировать и классифицирует риски, возникающие при защите информации, выбирает методы их расчётов

Практическая работа № 1-3.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ СЭД

Раздел 1. Современные электронные системы управления и работы с документами.

Тема 2. Сравнительный анализ возможностей современных СЭД

1. Цель занятия

1. Приобретение практических навыков анализа систем электронного документооборота
2. Приобретение практических навыков определения приоритетных направлений при анализе информационной системы.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвященный системам электронного делопроизводства.
2. Ознакомиться с заданием на практическое занятие.
3. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 10 мин.

Основная часть 160 мин.

Заключительная часть 10 мин.

Программа практического занятия:

1. Тестовый опрос по материалам лекции 1.
2. Решение ситуационных заданий:
 - выбор 6-8 СЭД для анализа;
 - проведение сравнительного анализа современных СЭД по следующим критериям: порядок регистрации документов; ведение регистрационной карточки; ведение номенклатуры дел; распознавание документов; работа со словарями;
 - Проведение сравнительного анализа СЭД по следующим критериям: поиск документов; ведение архивов; маршрутизация; генерация отчетов; интерфейс; интеграция с электронной почтой.

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- Выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

В комплекте с персональными ЭВМ

7. Основные теоретические сведения

2.1.5 Выбор системы защищённого электронного документооборота для организации

СЭД - это в первую очередь система, позволяющая решать все типовые задачи электронного документооборота для работы с документами — регистрация и ввод документов, поиск документов, маршрутизация, создание отчётов, ведение архива, установление прав доступа в системе. Поэтому при выборе СЭД просто необходимо убедиться в том, что система действительно обеспечивает выполнение таких задач. Чтобы получить представление о возможностях систем, позволяющих организовать электронный документооборот, была составлена таблица с необходимым набором функционала (таблица 1).

Таблица 1 - Основные возможности систем электронного документооборота

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Регистрация документов	+	+	+	+	+	+	+	+	+	+
Ведение РК	+	+	+	+	+	+	+	+	+	+
Ведение номенклатуры дел	+	+	+	+	+	+	+	+	+	+
Сканирование	+/-	+	+/-	+	+/-	+/-	+	+	+	+/-
Распознавание документов	+/-	+	+/-	+	+/-	+/-	+/-	+/-	+/-	+/-
Связанные документы	+	+	+	+	+	+	+	+	+	+
Прикрепленные файлы	+	+	+	+	+	+	+	+	+	+
Работа со словарями и справочниками	+	+	+	+	+	+	+	+	+	+
Сроки поручений	+	-	+	+	+	+	+	+	+	+
Поиск	+	+	+	+	+	+	+	+	+	+
Списание в архив	+	+	+	+	+	+	-	+	+	+
Ведение архивов	+/-	-	+/-	+/-	+/-	+/-	-	+/-	+/-	+/-
Маршрутизация	+	-	+	+	+	+	-	+	+	+
Генерация отчетов	+	+	+	+	+	+	+	+	+	+
Разграничение прав доступа	+	-	+/-	+	+	+	+	+	+	+

Как показано в таблице, все представленные системы стараются идти в ногу со временем и поэтому обладают почти всеми необходимыми функциональными возможностями. Наилучшим образом с типовыми задачами электронного документооборота справляются системы Дело, ЕВФРАТ-Документооборот,

DocsVision и LanDocs.

Для полноценной работы с системой в первую очередь необходимо пройти обучение. Разработчик должен предоставить постоянно действующую оперативную техническую поддержку. Услуги по установке и настройке системы, предлагаемые разработчиками, являются необязательными и могут понадобиться только в том случае, если собственные IT-специалисты не в силах самостоятельно осуществить адаптацию системы и ввод ее в эксплуатацию.

Суммарные затраты на приобретение системы складываются из стоимости лицензий программного продукта, базы данных, услуг, дополнительных модулей системы и стороннего программного обеспечения. По общей стоимости серверной и пользовательских лицензий, а также стоимости СУБД/платформы, наиболее приемлемыми являются системы ГранДок, ЕВФРАТ-Документооборот и DocsVision. Стоимость базы данных и программных платформ варьируется от 900 до 4000\$. Исключением является система ЕВФРАТ-Документооборот, имеющая встроенную СУБД Ника (таблица 4). Сравнение полных затрат на внедрение систем практически неосуществимо в силу различного подхода компаний-разработчиков к предоставлению услуг. В примечаниях к таблицам можно найти информацию об используемых системами базах данных и платформах, а также о модулях, стоимость которых учтена для систем LanDocs и CompanyMedia.

Таблица 2 - Стоимость сервера и лицензий

Система/Характеристика	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Стоимость СУБД, уе	От 3964	От 900	От 900	-	От 3964	От 900	От 900	От 900	От 900	От 900

Приобретая систему, не следует забывать о процессе ее внедрения и промышленной эксплуатации. Может оказаться, что все достоинства функционала приобретенной системы сойдут на «нет», когда дело дойдет до внедрения и использования системы. Например, если приобретаемая система не содержит инструментария необходимого для настройки под потребности организации собственными силами, то процесс внедрения будет требовать участия разработчика, что существенно повлияет на повышение стоимости внедрения. Адаптировать систему под нужды своей организации доступными средствами без участия разработчика и без дополнительных затрат смогут обладатели систем ЕВФРАТ-Документооборот и DocsVision.

Заказчикам других систем предлагается набор стандартных настроек, которые могут быть доработаны разработчиками или их партнерами, что приведет к увеличению затрат (таблица 3).

Таблица 3 - Доступный инструментарий для настройки системы

Система/инструментарий	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Дизайнер форм и карточек документов	+	-	+/-	+	+/-	+/-	-	+	+/-	+
Дизайнер маршрутов/процессов	+	-	+/-	+	+/-	+/-	-	+	+	+
Редактор отчетов	+/-	+/-	-	+	+/-	+/-	+/-	+	+	+/-
Создание и изменение словарей и	+	+	-	+	+	+/-	-	+	+	+

справочников										
--------------	--	--	--	--	--	--	--	--	--	--

Предполагая, что внедрение прошло успешно, следует рассмотреть, что же ещё существенно для автоматизации электронного документооборота. Помимо необходимого набора возможностей (таблица 3) наличие в системе дополнительного функционала (таблица 6) может значительно упростить работу с системой всем сотрудникам организации (например, настройка уведомлений и напоминаний). В некоторых случаях этот функционал просто необходим (например, WEB-доступ). Потребности заказчика в автоматизации процессов обработки документов со временем могут меняться (например, в случае изменения организационной структуры предприятия), что может привести к необходимости в развитии системы. Например, возникает ситуация, когда заказчик, успешно эксплуатирующий систему в головном офисе организации, впоследствии принимает решение о внедрении ее в филиалы. Как видно из таблицы 4, наиболее полноценный дополнительный функционал за счет гибких настроек пользовательского интерфейса предоставляют системы Босс-Референт и Optima-Workflow. По остальным параметрам уверенные позиции занимают системы Directum, DocsVision и ЕВФРАТ-Документооборот.

Таблица 4 - Дополнительные возможности работы с системой

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Настройка интерфейса	+	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+
Настройка уведомлений	+	+/-	+/-	+	+	+	+/-	+	+	+
Интеграция с электронной почтой	+	-	+/-	+	+	+	+/-	+	+/-	+
Web-доступ	+	-	+/-	+	+/-	+/-	+	+	+/-	+
Территориально-распределенная работа	+	-	-	+	+	+/-	+	+/-	+/-	+
Наличие API	+	-	+	+	+	+	-	+	+	+

Важными характеристиками СЭДО являются её безопасность, надёжность и производительность (таблица 7). Из таблицы 7 следует, что системы Directum, DocsVision, Optima-Workflow и ЕВФРАТ-Документооборот позволяют обеспечить необходимый уровень надёжности и безопасности СЭДО. В случае создания распределенной СЭДО количество одновременно работающих пользователей может измеряться тысячами. Хочется отметить, что системы Босс-Референт и CompanyMedia, реализованные на платформе Lotus Notes/Domino, предлагают наиболее развитые средства администрирования при распределенной работе за счет возможностей платформы.

Таблица 5 – Надёжность, безопасность

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Авторизация пользователей с паролем	+	+	+	+	+	+	+	+	+	+
Шифрование документов	+/-	-	+/-	+	+/-	+	+	+	+/-	+
Поддержка ЭЦП	+/-	+	+/-	+	+/-	+	+	+	+/-	+
Резервное копирование БД	+	-	+	+	+	+	-	+	+	+

Протокол событий	+	+/-	+	+	+	+	+	+	+	+
------------------	---	-----	---	---	---	---	---	---	---	---

Проанализировав рынок программных продуктов электронного документооборота, по представленным критериям, необходимо выбрать 4,5 наиболее приемлемых системы.

8. Литература

1. Некраха А.В., Шевцова Г.А. Организация конфиденциального делопроизводства. – М.: Академический проект, 2013. – 224 с.
2. Бутакова А.В., Семененко В.П. Защита и обработка конфиденциальных документов. – М.: Московский технологический институт, 2013. – 238 с.
3. Корнеев И. К., Степанов Е. А. Защита информации в офисе. – М.: Проспект, 2014. – 336 с.

Практическая работа № 4-6.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КАЧЕСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ СЭД

1. Цель занятия

1. Приобретение практических навыков анализа систем электронного документооборота
2. Приобретение практических навыков определения приоритетных направлений при анализе информационной системы.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый системам электронного делопроизводства.
2. Ознакомиться с заданием на практическое занятие.
3. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 10 мин

Основная часть 70 мин

Заключительная часть 10 мин

Программа практической работы

1. Тестовый опрос по материалам лекции
 2. Решение ситуационных заданий
 - выбор 6-8 СЭД для анализа;
 - проведение сравнительного анализа по критериям: регистрация обращений к базам и файлам; авторизация пользователей; сопровождение программного продукта;
 - защита информации при работе в интернет;
 - шифрование документов;
 - поддержка электронной цифровой подписи;
 - резервное копирование баз данных.
- Защита отчёта.

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- Выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

В комплекте с персональными ЭВМ

7. Основные теоретические сведения

2.1.5 Выбор системы защищённого электронного документооборота для организации

СЭД - это в первую очередь система, позволяющая решать все типовые задачи электронного документооборота для работы с документами — регистрация и ввод документов, поиск документов, маршрутизация, создание отчётов, ведение архива, установление прав доступа в системе. Поэтому при выборе СЭД просто необходимо убедиться в том, что система действительно обеспечивает выполнение таких задач. Чтобы получить представление о возможностях систем, позволяющих организовать электронный документооборот, была составлена таблица с необходимым набором функционала (таблица 1).

Таблица 1 - Основные возможности систем электронного документооборота

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Регистрация документов	+	+	+	+	+	+	+	+	+	+
Ведение РК	+	+	+	+	+	+	+	+	+	+
Ведение номенклатуры дел	+	+	+	+	+	+	+	+	+	+
Сканирование	+/-	+	+/-	+	+/-	+/-	+	+	+	+/-
Распознавание документов	+/-	+	+/-	+	+/-	+/-	+/-	+/-	+/-	+/-
Связанные документы	+	+	+	+	+	+	+	+	+	+
Прикрепленные файлы	+	+	+	+	+	+	+	+	+	+
Работа со словарями и справочниками	+	+	+	+	+	+	+	+	+	+
Сроки поручений	+	-	+	+	+	+	+	+	+	+
Поиск	+	+	+	+	+	+	+	+	+	+
Списание в архив	+	+	+	+	+	+	-	+	+	+
Ведение архивов	+/-	-	+/-	+/-	+/-	+/-	-	+/-	+/-	+/-
Маршрутизация	+	-	+	+	+	+	-	+	+	+
Генерация отчетов	+	+	+	+	+	+	+	+	+	+
Разграничение прав доступа	+	-	+/-	+	+	+	+	+	+	+

Как показано в таблице, все представленные системы стараются идти в ногу со временем и поэтому обладают почти всеми необходимыми функциональными возможностями. Наилучшим образом с типовыми задачами электронного документооборота справляются системы Дело, ЕВФРАТ-Документооборот, DocsVision и LanDocs.

Для полноценной работы с системой в первую очередь необходимо пройти обучение. Разработчик должен предоставить постоянно действующую оперативную техническую поддержку. Услуги по установке и настройке системы, предлагаемые разработчиками, являются необязательными и могут понадобиться только в том случае, если собственные ИТ-специалисты не в силах самостоятельно осуществить адаптацию

системы и ввод ее в эксплуатацию.

Суммарные затраты на приобретение системы складываются из стоимости лицензий программного продукта, базы данных, услуг, дополнительных модулей системы и стороннего программного обеспечения. По общей стоимости серверной и пользовательских лицензий, а также стоимости СУБД/платформы, наиболее приемлемыми являются системы ГранДок, ЕВФРАТ-Документооборот и DocsVision. Стоимость базы данных и программных платформ варьируется от 900 до 4000\$. Исключением является система ЕВФРАТ-Документооборот, имеющая встроенную СУБД Ника (таблица 4). Сравнение полных затрат на внедрение систем практически неосуществимо в силу различного подхода компаний-разработчиков к предоставлению услуг. В примечаниях к таблицам можно найти информацию об используемых системами базами данных и платформах, а также о модулях, стоимость которых учтена для систем LanDocs и CompanyMedia.

Таблица 2 - Стоимость сервера и лицензий

Система/Характеристика	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Стоимость СУБД, уе	От 3964	От 900	От 900	-	От 3964	От 900	От 900	От 900	От 900	От 900

Приобретая систему, не следует забывать о процессе ее внедрения и промышленной эксплуатации. Может оказаться, что все достоинства функционала приобретенной системы сойдут на «нет», когда дело дойдет до внедрения и использования системы. Например, если приобретаемая система не содержит инструментария необходимого для настройки под потребности организации собственными силами, то процесс внедрения будет требовать участия разработчика, что существенно повлияет на повышение стоимости внедрения. Адаптировать систему под нужды своей организации доступными средствами без участия разработчика и без дополнительных затрат смогут обладатели систем ЕВФРАТ-Документооборот и DocsVision.

Заказчикам других систем предлагается набор стандартных настроек, которые могут быть доработаны разработчиками или их партнерами, что приведет к увеличению затрат (таблица 3).

Таблица 3 - Доступный инструментарий для настройки системы

Система/инструментарий	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Дизайнер форм и карточек документов	+	-	+/-	+	+/-	+/-	-	+	+/-	+
Дизайнер маршрутов/процессов	+	-	+/-	+	+/-	+/-	-	+	+	+
Редактор отчетов	+/-	+/-	-	+	+/-	+/-	+/-	+	+	+/-
Создание и изменение словарей и справочников	+	+	-	+	+	+/-	-	+	+	+

Предполагая, что внедрение прошло успешно, следует рассмотреть, что же ещё существенно для автоматизации электронного документооборота. Помимо необходимого набора возможностей (таблица 3) наличие в системе дополнительного функционала (таблица 6) может значительно упростить работу с системой всем сотрудникам организации (например, настройка уведомлений и напоминаний). В некоторых случаях этот функционал просто необходим (например, WEB-доступ). Потребности заказчика в автоматизации процессов обработки документов со временем могут меняться (например, в случае изменения организационной структуры предприятия), что может привести к необходимости в развитии системы. Например, возникает ситуация, когда заказчик, успешно эксплуатирующий систему в головном офисе организации, впоследствии принимает решение о внедрении ее в филиалы. Как видно из таблицы 4, наиболее полноценный дополнительный функционал за счет гибких настроек пользовательского интерфейса предоставляют системы Босс-Референт и Optima-Workflow. По остальным параметрам уверенные позиции занимают системы Directum, DocsVision и ЕВФРАТ-Документооборот.

Таблица 4 - Дополнительные возможности работы с системой

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Настройка интерфейса	+	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+
Настройка уведомлений	+	+/-	+/-	+	+	+	+/-	+	+	+
Интеграция с электронной почтой	+	-	+/-	+	+	+	+/-	+	+/-	+
Web-доступ	+	-	+/-	+	+/-	+/-	+	+	+/-	+
Территориально-распределенная работа	+	-	-	+	+	+/-	+	+/-	+/-	+
Наличие API	+	-	+	+	+	+	-	+	+	+

Важными характеристиками СЭДО являются её безопасность, надёжность и производительность (таблица 7). Из таблицы 7 следует, что системы Directum, DocsVision, Optima-Workflow и ЕВФРАТ-Документооборот позволяют обеспечить необходимый уровень надёжности и безопасности СЭДО. В случае создания распределенной СЭДО количество одновременно работающих пользователей может измеряться тысячами. Хочется отметить, что системы Босс-Референт и CompanyMedia, реализованные на платформе Lotus Notes/Domino, предлагают наиболее развитые средства администрирования при распределенной работе за счет возможностей платформы.

Таблица 5 – Надёжность, безопасность

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Авторизация пользователей с паролем	+	+	+	+	+	+	+	+	+	+
Шифрование документов	+/-	-	+/-	+	+/-	+	+	+	+/-	+
Поддержка ЭЦП	+/-	+	+/-	+	+/-	+	+	+	+/-	+
Резервное копирование БД	+	-	+	+	+	+	-	+	+	+
Протокол событий	+	+/-	+	+	+	+	+	+	+	+

Проанализировав рынок программных продуктов электронного документооборота, по представленным критериям, необходимо выбрать 4,5 наиболее приемлемых системы.

8. Литература

- Некраха А.В., Шевцова Г.А. Организация конфиденциального делопроизводства. – М.: Академический проект, 2013. – 224 с.
- Бутакова А.В., Семененко В.П. Защита и обработка конфиденциальных документов. – М.: Московский технологический институт, 2013. – 238 с.
- Корнеев И. К., Степанов Е. А. Защита информации в офисе. – М.: Проспект, 2014. – 336 с.

9. Методические рекомендации по выполнению лабораторной работы

Провести сравнительный анализ качества защиты информации СЭД, указанных преподавателем, по выбранным критериям.

Информационная безопасность	DIRECTUM	БОСС-РЕФЕРЕНТ	ДЕЛО	ЕВФРАТ	МОТИВ
Поддержка различных способов аутентификации	0,5	1	0,5	0,5	0,5
Назначение прав пользователям	1	1	1	1	1
Назначение прав группам пользователей	1	1	1	0,5	0,5
Поддержка пользовательских ролей	1	1	1	1	1
Разграничение прав доступа к объектам системы (папка/вид РКК экземпляр РКК)	0,5	1	1	0,5	1
Разграничение прав доступа к операциям на уровне РКК прикрепленных файлов/реквизита	0,5	1	1	0,5	0
Выдача прав на время исполнения поручения/документа	1	0,5	1	1	0
Шифрование данных системы, шифрование данных при передаче	1	1	1	1	1
Протоколирование действий пользователей	1	1	1	1	1
Средства мониторинга событий в системе	0,5	1	0,5	1	1
Использование ЭЦП	1	1	1	1	1
Применение сертифицированных средств криптозащиты	1	1	1	1	1
Динамическая блокировка документа	1	0,5	1	1	1
Наличие программных средств контроля целостности документов	0	0	0	0,5	0
Организация резервного копирования базы данных	1	1	1	1	1
ИТОГО	12	13	13	12,5	11

10. Содержание отчета

По результатам выполнения лабораторной работы студенты оформляют и защищают отчёт в индивидуальном порядке в форме беседы.

Практическая работа № 7-9.

ОЦЕНКА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЭД

Раздел 2. Основные угрозы информации в системах электронного документооборота и способы борьбы с ними

Тема 7. Оценка риска информационной безопасности СЭД.

1. Цель занятия

1. Приобретение практических навыков анализа систем электронного документооборота
2. Приобретение практических навыков оценки уровня защищённости информационной системы.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал, посвящённый системам электронного делопроизводства.
2. Ознакомиться с заданием на практическое занятие.
3. Ответить на контрольные вопросы.

3. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 10 мин

Основная часть 160 мин

Заключительная часть 10 мин.

Программа лабораторной работы:

1. Тестовый опрос по материалам лекции 10.
2. Решение ситуационных заданий:
 - анализ структуры и деятельности предприятия;
 - определение перечня ценной информации на предприятии;
 - определение актуальных угроз и вероятностей их реализации;
 - определение степени использования нормативных документов по защите информации;
 - определение коэффициента использования организационных и технических средств защиты информации;
 - количественная оценка величины риска информационной безопасности предприятия;
 - анализ результатов расчётов.

4. Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

4.1. Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

4.2. Требования безопасности во время работы

- Выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию.
- Подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса.
- При обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

4.3. Требования безопасности по окончании работы

- Доложить руководителю занятий или лаборанту о завершении работ.
- Привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

5. Аппаратное обеспечение

Класс персональных ЭВМ, классная доска, мел (маркеры).

6. Программное обеспечение

В комплекте с персональными ЭВМ

7. Основные теоретические сведения

7.1 Методика количественной оценки риска ИБ информационной системы

Назначение методики

Настоящая методика предназначена для проведения оценки рисков информационной безопасности (ИБ) в рамках построения или совершенствования системы информационной безопасности на предприятиях малого и среднего бизнеса.

Настоящая методика рекомендована для применения путем прямого использования устанавливаемых в ней положений при проведении оценки рисков ИБ и использовании результатов оценки рисков ИБ.

Постановка задачи

Основная задача данной методики заключается в том, чтобы определить численный показатель риска ИБ с целью принятия эффективных мер по защите информации. Предлагаемая методика оценки рисков позволяет выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

Обобщенный алгоритм проведения оценки рисков ИБ на предприятиях малого и среднего бизнеса (далее МСБ) приведен на рис. 1.

Этапы	Название этапов
Этап 1	Идентификация активов
Этап 2	Определение риска несоответствия требованиям законодательства
Этап 3	Разработка модели угроз
Этап 4	Количественное определение риска
Этап 5	Определение допустимого уровня риска

Рисунок 1– Алгоритм оценки риска ИБ

Процедуры оценки рисков ИБ как комплексного подхода выполняются сотрудниками предприятия совместно с руководящим звеном, а также с сотрудниками отделов предприятия.

Этап 1. Идентификация активов. На данном этапе эксперты проводят интервью с персоналом каждого подразделения или отдела с целью выявления используемых активов. Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую вкладывает средства и которые, соответственно, требует защиты со стороны предприятия. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение. Описание информационных активов проводится путём построения бинарных высказываний (описывалась в более ранних статьях) Могут существовать следующие типы активов:

1. Информация/данные (например, файлы, содержащие информацию о платежах или продукте).
2. Аппаратные средства (например, компьютеры, принтеры).
3. Программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения).
4. Оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели).
5. Программно-аппаратные средства (например, электронные носители информации).
6. Документы (например, контракты).
7. Продукция предприятия.
8. Услуги (например, информационные, вычислительные услуги).
9. Конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей).
10. Оборудование, обеспечивающее необходимые условия работы.

11. Персонал организации.
12. Престиж (имидж) организации.

Этап 2. Определение риска несоответствия требований законодательства в области ИБ. Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ МСБ. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0».

Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются.

В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ, который определяется по табл. 1.

Таблица 1

Сумма Выполненных требований	Риск несоответствия требованиям законодательства (R_n)
40–51	0,01
27–39	0,25
Менее 26	0,5
Не выполняются	0,9

Этап 3. Разработка модели угроз.

В методике с целью максимально точного определения риска ИБ необходимо разработать частную модель угроз ИБ предприятию. В модели угроз предлагается использовать уже разработанный и описанный в более ранних статьях метод оценки угроз с использованием алгоритма логического вывода Сорит. Определение вероятности наступления неблагоприятных событий определяется экспертом или группой экспертов, занимающихся разработкой модели угроз. Экспертным методом определяется и актуальность угроз ИБ.

После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или групп активов, подверженных этим угрозам, а также определяют вероятность реализации угроз. Весь процесс составления перечня актуальных угроз проводится с использованием теории графов, с помощью которой описывается методика актуализации угроз.

Этап 4. Процедура количественной оценки рисков ИБ. Основным этапом в процессе оценки рисков является процедура количественного определения рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен на рис. 2.



Рисунок 2. Алгоритм количественного оценивания риска ИБ

Процедура количественной оценки рисков ИБ включает в себя следующие шаги:

Шаг 1. Выбор актуальных угроз частной модели угроз. На данном шаге, используя частную модель угроз, формируется перечень актуальных угроз ИБ активов предприятия. На данном шаге количественного оценивания рисков сопоставляются идентифицированные активы с направленными на них угрозами. Для этого используется перечень активов предприятия и каждому из них сопоставляются актуальные угрозы из модели угроз.

Шаг 2. Определение вероятности наступления угрозы. В связи с тем, что на один актив могут воздействовать одновременно несколько угроз, необходимо определить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу.

Определение вероятности наступления неблагоприятных событий в связи с реализацией хотя бы одной угрозы из перечня актуальных угроз на рассматриваемый актив. Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз $P_{y1}, P_{y2}, \dots, P_{yn}$, где n – количество угроз, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

$$P_{ygr} = 1 - \Pi(1 - P_{y1})(1 - P_{y2})(1 - P_{y3})\dots(1 - P_{yn}), \text{ где } n\text{-количество угроз}$$

Шаг 3. Определение ценности актива. Ценность актива определяется стоимостью информационного актива. В связи с тем, что зачастую невозможно определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса.

Шаг 4. Определение возможности использования организационных и технических уязвимостей.

Возможность использования организационных уязвимостей проводится экспертным методом, анализируя применяемые организационные меры защиты информации. В ходе проведения анализа, всем организационным мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В табл. 2 представлены соответствие выполняемых организационных мер защиты информации и коэффициент уязвимости организационных мер защиты информации.

Таблица 2

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_o)
14–17	0,01
8-13	0,25
Менее 8	0.5
Не выполняются	0,9

Возможность использования технических уязвимостей проводится экспертным методом, анализируя применяемые технические меры защиты информации. В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В табл. 3 представлено соответствие выполняемых технических мер защиты информации и коэффициент уязвимости технических мер защиты информации.

Таблица 3

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_t)
15-19	0.01
9-14	0.25
Менее 9	0.5
Не выполняются	0.9

Шаг 5. Вычисление численного значения риска. В разрабатываемой методике процедура оценки рисков реализации хотя бы одной угрозы основывается на взаимности нескольких факторов – вероятности

происшествия, а именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу.

В настоящей методике процедура количественной оценки рисков реализации хотя бы одной угрозы из всего перечня актуальных угроз по отношению к конкурентному активу определяется относительно каждого типа актива, на который воздействует совокупность угроз ИБ, что позволяет дискретно определить риск наступления неблагоприятных событий на каждый тип актива.

Общая формула (1) определения риска реализации хотя бы одной угрозы из всего перечня актуальных угроз с учетом наличия уязвимостей по отношению

$$R = P_{\text{угр}} R_n C \frac{K_o + K_t}{2} 100 \% , \quad (1)$$

где R – численная величина риска реализации угроз ИБ;

$P_{\text{угр}}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз; R_n – риск несоответствия требованиям законодательства;

C – ценность актива (0...1);

K_o – вероятность использования организационных уязвимостей;

K_t – вероятность использования технических уязвимостей.

Этап 5. Определение допустимого уровня риска.

Допустимый риск принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для предприятия МСБ рекомендованное значение риска не должно превышать 5%. Это обуславливается в первую очередь тем, что максимальная выручка предприятий МСБ за отчетный период, например 1 год, может составлять до 400 млн рублей, это из расчета того, что в случае реализации одной из актуальных угроз, может повлечь убыток в размере более 5% выручки, является недопустимым и требующим принятия эффективных мер.

Заключение

Выполнение всех этапов проведения оценки рисков ИБ на предприятиях МСБ повторяется для каждого типа актива.

Полученное значение рисков ИБ необходимо для выработки рекомендаций по снижению уровня риска, а также принятия эффективных мер по обеспечению ИБ предприятия. В случае если итоговое значение риска менее 5%, то делается вывод о том, что на предприятии выполнены требования по ИБ в полной необходимости, а также что риск ИБ оцениваемого типа актива допустимый. Но необходимо периодически проводить переоценку рисков ИБ. В случае если итоговое значение риска более или равно 5%, то делается вывод о том, что на предприятии не выполняются требования по ИБ, а также что риск ИБ оцениваемого типа актива повышенный и требует немедленного принятия решений.

8. Литература

7. Некрах А.В., Шевцова Г.А. Организация конфиденциального делопроизводства. – М.: Академический проект, 2013. – 224 с.
8. Бутакова А.В., Семененко В.П. Защита и обработка конфиденциальных документов. – М.: Московский технологический институт, 2013. – 238 с.
9. Корнеев И. К., Степанов Е. А. Защита информации в офисе. – М.: Проспект, 2014. – 336 с.

9. Методические рекомендации по выполнению лабораторной работы

Провести оценку риска информационной безопасности систем электронного документооборота по вариантам заданным преподавателям.

10. Содержание отчета о лабораторной работе

По результатам выполнения лабораторной работы студенты оформляют отчет и защищают его в индивидуальном порядке в форме беседы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Методы и средства защиты информации
в системах электронного документооборота»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль):
«Информационная безопасность киберфизических систем»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ПРАКТИЧЕКАЯ РАБОТА № 1-3.	5
2.1.5 ВЫБОР СИСТЕМЫ ЗАЩИЩЁННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ ОРГАНИЗАЦИИ	6
ПРАКТИЧЕКАЯ РАБОТА № 4-6.	10
2.1.5 ВЫБОР СИСТЕМЫ ЗАЩИЩЁННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ ОРГАНИЗАЦИИ	11
ПРАКТИЧЕСКАЯ РАБОТА № 7-9.	15
7.1 МЕТОДИКА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКА ИБ ИНФОРМАЦИОННОЙ СИСТЕМЫ	16
ВВЕДЕНИЕ	22
1. ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА	22
2. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ДИСЦИПЛИНЕ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»	23
ПОЯСНИТЕЛЬНАЯ ЗАПИСКА	24
ПЛАН-ГРАФИК ВЫПОЛНЕНИЯ СРС ПО ДИСЦИПЛИНЕ	24
ЗАДАНИЯ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ	25
1.1 Порядок выполнения задания	25
3.1.1 Обзор отечественных систем электронного делопроизводства	25
3.1.2 Сравнительный анализ качества защиты информации в современных СЭД.	28
3.1.3 Оценка риска информационной безопасности СЭД.	31
3.1.4 Электронная цифровая подпись в системе электронного делопроизводства.	33
3.1.5 Модули и основные функции системы электронного делопроизводства «Дело»	35
3.1.6 Порядок выбора системы электронного документооборота	36
АЛГОРИТМ РАБОТЫ ПО ВЫБОРУ СИСТЕМЫ ЗАЩИЩЁННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	36
ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К БУДУЩЕЙ СИСТЕМЕ ЭЛЕКТРОННОГО ЗАЩИЩЁННОГО ДОКУМЕНТООБОРОТА	37
3.1.7 Работа с модулями СЭД «Дело»	37
КРАТКИЕ СВЕДЕНИЯ ИЗ ТЕОРИИ	38
Работа над проектами документов	43
Контроль за исполнением поручений (документов)	45
Исполнение поручений (документов)	45
Организация документооборота	46
Списание документов в дело	46
ПОСЛЕ ИСПОЛНЕНИЯ ДОКУМЕНТА ОН СПИСЫВАЕТСЯ В ДЕЛО. СПИСАНИЕ ДОКУМЕНТА В ДЕЛО ОСУЩЕСТВЛЯЕТСЯ ПУТЕМ ЗАНЕСЕНИЯ В РК ЗАПИСИ, СОДЕРЖАЩЕЙ НАИМЕНОВАНИЕ ДЕЛА (СОГЛАСНО СПРАВОЧНИКУ "НОМЕНКЛАТУРА ДЕЛ"), ДАТУ И ВРЕМЯ СПИСАНИЯ. СПРАВОЧНИК "НОМЕНКЛАТУРА ДЕЛ" ЗАПОЛНЯЕТСЯ СИСТЕМНЫМ ТЕХНОЛОГОМ В СООТВЕТСТВИИ С ЕЖЕГОДНО УТВЕРЖДАЕМОЙ НОМЕНКЛАТУРОЙ	46
КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ РАБОТЫ	46
3.1.8 Оценка эффективности систем электронного документооборота.	46
4. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ	49
4.1 ОСНОВНАЯ ЛИТЕРАТУРА	49
4.2 ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	49

Введение

Основной целью изучения дисциплины «Управление информационной безопасностью» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 Информационная безопасность.

Для достижения указанной цели в процессе изучения данной дисциплины необходимо решить следующие задачи:

- приобретение студентами теоретических знаний по системному подходу к управлению информационной безопасностью и практических навыков по их моделированию.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

№ п/п	Содержание компетенции	Шифр
Общепрофессиональные компетенции		ОК-(№)
1.	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ОПК-3

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ	– современные подходы к управлению ИБ и направлениях их развития; – основные стандарты, регламентирующие управление ИБ; – принципы построения СУИБ; – принципы разработки процессов управления ИБ;
УМЕТЬ	– анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; – определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; – применять процессный подход к управлению ИБ в различных сферах деятельности;
ВЛАДЕТЬ	– навыками управления информационной безопасностью простых объектов; – терминологией и процессным подходом построения систем управления ИБ; – навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области управления информационной безопасностью. На лабораторных занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям и тестовые задания, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью выяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой

частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Управление информационной безопасностью»

Коды реализуемых компетенций, индикаторов	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
4 семестр					
ИД-2 _{ОПК-3} ИД-3 _{ОПК-3}	Подготовка к лабораторной работе	Собеседование	16.00	2.00	18.00
ИД-1 _{ОПК-1} , ИД-3 _{ОПК-1} , ИД-2 _{ОПК-3} ИД-3 _{ОПК-3}	Самостоятельное изучение литературы	Собеседование	16.00	2.00	18.00
Итого за 1 семестр			32.00	4.00	36.00
Итого			32.00	4.00	36.00

Пояснительная записка

Обучение имеет целью не только дать студентам глубокие знания по дисциплине, но и научить их самостоятельно работать с литературой и информационными источниками.

Самостоятельная работа студентов является определяющим фактором их успешного обучения.

Время на самостоятельную работу рассчитывается примерно исходя из 4 часов ежедневной самостоятельной работы студента.

Преподаватель организует самостоятельную работу студентов по дисциплине путем:

- рекомендации студентам наиболее рациональных методов самостоятельного изучения учебного материала;

- организации изучения опыта самостоятельной работы студентов над учебным материалом, его обобщения и принятие действенных мер к повышению эффективности самостоятельной работы студентов;

- контроля самостоятельной работы студентов при проведении всех видов занятий, выборочной проверки конспектов лекций, а также путем индивидуального собеседования;

- оказания помощи отдельным студентам в овладении учебным материалом во время консультаций;

Консультации являются одной из форм работы кафедры по оказанию педагогически целесообразной помощи студентам в их самостоятельной работе.

Консультации должны носить индивидуальный характер. В случае необходимости разъяснения общих вопросов нескольким студентам проводятся групповые консультации.

Консультации проводятся с целью:

- разъяснения вопросов, возникающих у студентов при самостоятельном изучении учебного материала и выполнении домашних заданий;

- углубления и закрепления знаний по отдельным вопросам и темам дисциплины;

- оказания методической помощи в выборе методов самостоятельной работы.

Посещение консультаций студентов добровольное. Однако преподаватель может организовывать вызовы на собеседование тех студентов, которые в процессе обучения не показывают твердых знаний и не пользуются консультациями по своей инициативе.

На консультации преподаватель объясняет непонятные студентам наиболее сложные вопросы, и указывают литературу, в которой они освещаются.

План-график выполнения СРС по дисциплине

№	Название контрольной точки	Срок сдачи (номер недели)	Форма контроля	Срок консультации с преподавателем, номер недели
3 семестр				
1	Обзор отечественных систем электронного делопроизводства.	3	Компьютерное тестирование	3
2	Сравнительный анализ качества защиты информации в современных СЭД.	5	Защита отчёта по лабораторной работе	5
3	Оценка риска информационной безопасности СЭД.	7	Защита отчёта по лабораторной работе	7
4	Электронная цифровая подпись в системе электронного делопроизводства.	9	Компьютерное тестирование	9
5	Модули и основные функции системы электронного делопроизводства «Дело»	10	Компьютерное тестирование	10
6	Порядок выбора системы электронного документооборота.	12	Компьютерное тестирование	12
7	Работа с модулями СЭД «Дело»	14	Защита отчёта по лабораторной работе	14
8	Оценка эффективности систем электронного документооборота.	15	Компьютерное тестирование	15

Задания к самостоятельной работе

№	Название раздела (темы)	Цель	Форма контроля СРС	Задание для СРС	Требования к представлению и оформлению результатов	Рекомендуемая литература
1	Раздел 1. Современные электронные системы управления работы документами и с	ОК-2, ПК-10	Компьютерное тестирование	Обзор отечественных систем электронного делопроизводства.	Материал оформить в конспекте	[1],[3]
		ПК-14,16	Защита отчёта по лабораторной работе	Сравнительный анализ качества защиты информации в современных СЭД.	Оформить отчёт о лабораторной работе	[1],[3]
2	Раздел 2. Основные угрозы информации в системах электронного документооборота и способы борьбы с ними.	ПК- 14,16	Защита отчёта по лабораторной работе	Оценка риска информационной безопасности СЭД.	Оформить отчёт о лабораторной работе	[1],[2], [4]
		ПК- 14,16	Компьютерное тестирование.	Электронная цифровая подпись в системе электронного делопроизводства.	Материал оформить в конспекте	[2],[4]
3	Раздел 3. Порядок организации защищённого электронного документооборота на предприятии	ОК-2, ПК-10	Компьютерное тестирование	Модули и основные функции системы электронного делопроизводства «Дело»	Материал оформить в конспекте	[1],[3],[4],[5]
		ПК-10	Компьютерное тестирование	Порядок выбора системы электронного документооборота	Материал оформить в конспекте	[3],[6]
		ПК-14,16	Защита отчёта по лабораторной работе	Работа с модулями СЭД «Дело»	Оформить отчёт о лабораторной работе	[2],[3]
		ОК-2, ПК-10	Компьютерное тестирование	Оценка эффективности систем электронного документооборота	Материал оформить в конспекте	[5..6]

1.1 Порядок выполнения задания

3.1.1 Обзор отечественных систем электронного делопроизводства

Вопросы, подлежащие изучению:

- виды систем электронного делопроизводства;
- основные характеристики систем электронного делопроизводства
- обзор отечественных СЭД;

Краткие сведения из теории

Виды систем электронного делопроизводства

Система электронного документооборота может работать в одном из двух режимов:

- docflow (поток документов);
- workflow (поток работ)

В режиме docflow система ориентирована на обработку документов по одному: документ регистрируется в системе и далее может маршрутизироваться (передаваться от одного лица другому), согласовываться и т.д. Системы, работающие в данном режиме, как правило, ориентированы на

автоматизацию канцелярии, учёт резолюций и поручений.

Режим workflow позволяет автоматизировать бизнес-процессы предприятия. Бизнес-процесс — это набор шагов, которые необходимо выполнить, чтобы достичь результата. Бизнес-процесс может содержать ветвления и шаги, выполняемые только при определённых условиях, т.е. схему, согласно которой ставится задача сотруднику. И если для исполнения нужен один документ, то в компьютер к сотруднику в нужный момент поступит этот единственный документ. Если же нужно несколько документов, то придет несколько.

Рассмотрим, например, внешнюю экономическую деятельность. По одной сделке с иностранным партнёром требуется огромное количество документов. Список растянется страницы на три, и у каждого документа будут свои сроки разработки, свой жизненный цикл. Очевидно, что для такой деятельности подойдет только workflow-система.

Workflow-система может работать и с единичными документами, поддерживая более простой docflow-режим. Но если хотя бы один бизнес-процесс в работе компании требует "потока работ", то подойдет только workflow-система.

Многие производители систем электронного документооборота позиционируют свои продукты как workflow. Но выросли они из docflow и содержат ограничения, присущие этому режиму работы. Поэтому надо быть внимательным при изучении предлагаемых решений.

Основные характеристики систем электронного делопроизводства

Для решения тех проблем, которые указаны выше, крупные предприятия, прибегают к внедрению и использованию корпоративных информационных систем. Корпоративная информационная система - система, пользователем которой может быть только ограниченный круг лиц, определенный ее владельцем.

Одной из важнейших составляющих корпоративной информационной системы является СЭД.

Основные цели создания общекорпоративной СЭД:

- формирование единой политики и координирования работ в области электронного управления документами;

- выработка корпоративных стандартов работы с ЭД;
- эффективное управление документами в течение всего их жизненного цикла;
- оптимизация существующих деловых процессов;
- создание информационных порталов. СЭД, обладающие средствами совместной работы, дают возможность накапливать и использовать информацию в распределенной корпоративной среде на основе применения единых бизнес-правил, контекста и метаданных.

СЭД реализует следующие функции:

- управление жизненным циклом документа. Возможность управления документами в течение всего их жизненного цикла - от разработки, редакции, согласования, утверждения до распространения и архивирования;

- распределенная работа с документами. СЭД позволяет сотрудникам, работающим в различных территориально удаленных подразделениях, совместно использовать документы на локальных серверах, сохраняя при этом целостность документов в масштабе всей распределенной организации;

- широкий набор средств управления документами. СЭД обеспечивает все основные функции управления документами:

- а) регистрация документов;
- б) рассылка;
- в) постановка на контроль исполнения;
- г) контроль версий;
- д) полнотекстовый поиск;
- е) ведение контрольных журналов;
- ж) работа с шаблонами;
- з) уведомление об изменениях и другие;

- редактирование/согласование/утверждение. СЭД управляет всем интерактивным циклом редактирования и внесения изменений в документы вплоть до окончательного утверждения;

- многоуровневый контроль версий. Позволяет структурировать и хранить все черновики документов;

- защита данных. СЭД предоставляет мощные средства защиты данных:

- а) средства защиты и шифрования промышленного уровня;
- б) полномасштабные средства идентификации пользователей;
- в) средства RSA и SSL;

- поддержка широкого выбора клиентов. Возможность совместной работы в масштабах всей корпоративной сети с использованием для этого web-браузеров или клиентов Notes. Для доступа и сохранения документов в СЭД возможно использование файлов любых офисных приложений, совместных с протоколом ODMA;

- масштабируемость системы. Предусмотрена возможность внедрения системы с небольшого шага, а затем развертывание и наращивание функционала системы.

Ядро СЭД реализует стандартные процессы работы с входящими, исходящими и внутренними документами. Следовательно, для данного блока системы целесообразно использовать уже готовые программные решения [8].

СЭД призваны обеспечить следующие процессы: создание, управление доступом и распространение больших объемов документов в компьютерных сетях, а так же обеспечивала контроль над потоками документов организации. Часто эти документы хранятся в специальных хранилищах или в иерархии файловой системы. Типы файлов, которые, как правило, поддерживают СЭД, включают текстовые документы, образы, электронные таблицы, аудио-, видеоданные и документы Web. Общими возможностями СЭД является создание документов, управление доступом, преобразование и безопасность.

СЭД включают:

- системы электронного документирования;
- системы электронного документооборота;
- корпоративные СЭД.

Для обеспечения эффективной деятельности современных учреждений СЭД должны удовлетворять следующим требованиям:

- масштабируемость. Система должна поддерживать различное количество пользователей и ее способность наращивать мощность должна определяться только мощностью аппаратного обеспечения, на котором она установлена;
- распределенность. Архитектура системы должна поддерживать взаимодействие территориально распределенных структурных подразделений организации;
- модульность. Система ЭУД должна состоять из отдельных модулей, интегрированных между собой, что обеспечивает возможность поэтапного внедрения системы;
- открытость. Открытая архитектура системы позволяет, во-первых, быстро расширять платформу управления документами в ответ на появление новых бизнесцелей, во-вторых, интегрировать систему с другими прикладными программами, которые используются в организации, в-третьих, интегрировать управление документами с более широкими стратегическими инициативами, такими как управление знаниями;
- надежность. Система должна обладать техническими и программными средствами, обеспечивающими надежную и бесперебойную работу системы при различных видах сбоев;
- защищенность. Гибкость управления доступом ко всему спектру документов, от электронной почты до дискуссионных баз данных, от видеоклипов до формализованных документов всех типов;
- доступность. Возможность обеспечения доступа к документам через web-браузеры, настольные приложения и другие общедоступные типы клиентов;
- поддержка стандартов. Поддержка стандартов на различных этапах жизненного цикла электронного документа;
- комплексная функциональность (поддержка полного жизненного цикла работы с документами).

Классификация систем электронного управления документами представлена в таблице 3.

Таблица 3– Классификация систем электронного управления документами

Характеристика	Системы электронного документирования	Системы электронного документооборота	Корпоративные СЭД
Функциональное назначение	Обеспечивают работу с электронными версиями документов и реквизитами регистрационно-контрольных форм	Обеспечивают регламентированное и контролируемое движение ЭД внутри и вне организации на основе ИТ	Тоже в масштабах всей организации в целом
Динамика событий и процессов	Регистрация свершившихся событий (регистрация, хранение, контроль исполнения)	Регистрация свершившихся событий и действий, поддержка процессов работы над документами	Тоже в масштабах всей организации
Уровень автоматизации процессов	Системы, ориентированные на бизнес-процессы	Системы, ориентированные на бизнес-процессы с автоматизацией управления потоками работ	Системы, ориентированные на бизнес-процессы с автоматизацией

			управления потоками работ и поддержкой принятия решения
Пользователи	Сотрудники ограниченного числа структурных подразделений	Отдельные сотрудники многих подразделений, вовлеченные в какой-либо общий бизнес-процесс	Все сотрудники из различных подразделений организации, вовлеченные в бизнес-процессы масштаба всей организации

Обзор отечественных систем электронного делопроизводства

«МОТИВ» – автоматизированная система оперативного управления компанией относится к Web-ориентированным приложениям и является организующим инструментом управления для любой организации. Система содержит средства коллективной работы, позволяющие автоматизировать постановку поручений и задач, а также контроль их исполнения. Разработчиком системы «Мотив» является белгородская коммерческая организация **«Институт высоких технологий БелГУ»**.

NAUDOC – система управления корпоративной информацией через Web, разработанная компанией **NAUMEN** (ЗАО «Наумен», www.naumen.ru).

Система оптимальным образом подходит для автоматизации документооборота предприятий среднего и малого бизнеса, управляющих компаний, проектных организаций, подразделений холдинговых структур, а также для решения конкретных задач, встающих перед подразделениями больших компаний (обеспечение работы с нормативной документацией в соответствии с требованиями ISO 9000:2001, взаимодействие между сотрудниками и службой персонала и др.).

Особенностью системы является использование оригинальной архитектуры: язык разработки высокого уровня Python, позволяющий быстро реализовать бизнес-логику, и объектная база данных ZODB с открытыми исходными кодами.

OPTIMA-WorkFlow – комплексная система автоматизации управления потоками работ и организации конфиденциального документооборота является интегрированным аппаратно-программным решением, предназначенным для автоматизации создания и обработки вовлеченных в деловые процессы объектов или их электронных прототипов; для формирования правил и описания способов обработки и обеспечения доступа к ним пользователей со своих рабочих мест; для осуществления контроля над ходом выполнения работ над объектом и их результатами.

Основной принцип данной системы – это ориентированность ее на автоматизацию деловых процессов, управление потоками работ, организацию электронного документооборота, а не на действия, связанные с обработкой документов.

Контрольные вопросы для защиты работы:

- дать определение системам электронного делопроизводства и документооборота;
- классификационные признаки СЭД;
- основные функции СЭД;
- перечислить наиболее популярные СЭД в РФ;
- достоинства и недостатки СЭД;
- проблемы внедрения СЭД;
- перспективы развития СЭД.

3.1.2 Сравнительный анализ качества защиты информации в современных СЭД.

Вопросы, подлежащие изучению:

- выбор 6-8 СЭД для анализа;
- проведение сравнительного анализа по критериям: регистрация обращений к базам и файлам; авторизация пользователей; сопровождение программного продукта; защита информации при работе в интернет; шифрование документов; поддержка электронной цифровой подписи; резервное копирование баз

данных.

Краткие сведения из теории

СЭД - это в первую очередь система, позволяющая решать все типовые задачи электронного документооборота для работы с документами — регистрация и ввод документов, поиск документов, маршрутизация, создание отчетов, ведение архива, установление прав доступа в системе. Поэтому при выборе СЭД просто необходимо убедиться в том, что система действительно обеспечивает выполнение таких задач. Чтобы получить представление о возможностях систем, позволяющих организовать электронный документооборот, была составлена таблица с необходимым набором функционала (таблица 4). Таблица 4 - Основные возможности систем электронного документооборота

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Регистрация документов	+	+	+	+	+	+	+	+	+	+
Ведение РК	+	+	+	+	+	+	+	+	+	+
Ведение номенклатуры дел	+	+	+	+	+	+	+	+	+	+
Сканирование	+/-	+	+/-	+	+/-	+/-	+	+	+	+/-
Распознавание документов	+/-	+	+/-	+	+/-	+/-	+/-	+/-	+/-	+/-
Связанные документы	+	+	+	+	+	+	+	+	+	+
Прикрепленные файлы	+	+	+	+	+	+	+	+	+	+
Работа со словарями и справочниками	+	+	+	+	+	+	+	+	+	+
Сроки поручений	+	-	+	+	+	+	+	+	+	+
Поиск	+	+	+	+	+	+	+	+	+	+
Списание в архив	+	+	+	+	+	+	-	+	+	+
Ведение архивов	+/-	-	+/-	+/-	+/-	+/-	-	+/-	+/-	+/-
Маршрутизация	+	-	+	+	+	+	-	+	+	+
Генерация отчетов	+	+	+	+	+	+	+	+	+	+
Разграничение прав доступа	+	-	+/-	+	+	+	+	+	+	+

Как показано в таблице, все представленные системы стараются идти в ногу со временем и поэтому обладают почти всеми необходимыми функциональными возможностями. Наилучшим образом с типовыми задачами электронного документооборота справляются системы Дело, ЕВФРАТ-Документооборот, DocsVision и LanDocs.

Для полноценной работы с системой в первую очередь необходимо пройти обучение. Разработчик должен предоставить постоянно действующую оперативную техническую поддержку. Услуги по установке и настройке системы, предлагаемые разработчиками, являются необязательными и могут понадобиться только в том случае, если собственные ИТ-специалисты не в силах самостоятельно осуществить адаптацию системы и ввод ее в эксплуатацию.

Суммарные затраты на приобретение системы складываются из стоимости лицензий программного продукта, базы данных, услуг, дополнительных модулей системы и стороннего программного обеспечения. По общей стоимости серверной и пользовательских лицензий, а также стоимости СУБД/платформы, наиболее приемлемыми являются системы ГранДок, ЕВФРАТ-Документооборот и DocsVision. Стоимость базы данных и программных платформ варьируется от 900 до 4000\$. Исключением является система ЕВФРАТ-Документооборот, имеющая встроенную СУБД Ника (таблица 5). Сравнение полных затрат на внедрение систем практически неосуществимо в силу различного подхода компаний-разработчиков к предоставлению услуг. В примечаниях к таблицам можно найти информацию об используемых системами базами данных и платформах, а также о модулях, стоимость которых учтена для систем LanDocs и

Таблица 5 - Стоимость сервера и лицензий

Система/ Характеристика	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Стоимость СУБД, уе	От 3964	От 900	От 900	-	От 3964	От 900	От 900	От 900	От 900	От 900

Приобретая систему, не следует забывать о процессе ее внедрения и промышленной эксплуатации. Может оказаться, что все достоинства функционала приобретенной системы сойдут на «нет», когда дело дойдёт до внедрения и использования системы. Например, если приобретаемая система не содержит инструментария необходимого для настройки под потребности организации собственными силами, то процесс внедрения будет требовать участия разработчика, что существенно повлияет на повышение стоимости внедрения. Адаптировать систему под нужды своей организации доступными средствами без участия разработчика и без дополнительных затрат смогут обладатели систем ЕВФРАТ-Документооборот и DocsVision.

Заказчикам других систем предлагается набор стандартных настроек, которые могут быть доработаны разработчиками или их партнерами, что приведет к увеличению затрат (таблица 6).

Таблица 6 - Доступный инструментарий для настройки системы

Система/инструментарий	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Дизайнер форм и карточек документов	+	-	+/-	+	+/-	+/-	-	+	+/-	+
Дизайнер маршрутов/процессов	+	-	+/-	+	+/-	+/-	-	+	+	+
Редактор отчетов	+/-	+/-	-	+	+/-	+/-	+/-	+	+	+/-
Создание и изменение словарей и справочников	+	+	-	+	+	+/-	-	+	+	+

Предполагая, что внедрение прошло успешно, следует рассмотреть, что же ещё существенно для автоматизации электронного документооборота. Помимо необходимого набора возможностей (таблица 6) наличие в системе дополнительного функционала (таблица 7) может значительно упростить работу с системой всем сотрудникам организации (например, настройка уведомлений и напоминаний). В некоторых случаях этот функционал просто необходим (например, WEB-доступ). Потребности заказчика в автоматизации процессов обработки документов со временем могут меняться (например, в случае изменения организационной структуры предприятия), что может привести к необходимости в развитии системы. Например, возникает ситуация, когда заказчик, успешно эксплуатирующий систему в головном офисе организации, впоследствии принимает решение о внедрении ее в филиалы. Как видно из таблицы 5, наиболее полноценный дополнительный функционал за счет гибких настроек пользовательского интерфейса предоставляют системы Босс-Референт и Optima-Workflow. По остальным параметрам уверенные позиции занимают системы Directum, DocsVision и ЕВФРАТ-Документооборот.

Таблица 7 - Дополнительные возможности работы с системой

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	Д	DIS	DV	LD	O-W
Настройка интерфейса	+	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+
Настройка уведомлений	+	+/-	+/-	+	+	+	+/-	+	+	+
Интеграция с электронной почтой	+	-	+/-	+	+	+	+/-	+	+/-	+
Web-доступ	+	-	+/-	+	+/-	+/-	+	+	+/-	+
Территориально-распределенная работа	+	-	-	+	+	+/-	+	+/-	+/-	+
Наличие API	+	-	+	+	+	+	-	+	+	+

Важными характеристиками СЭДО являются её безопасность, надёжность и производительность (таблица 7). Из таблицы 7 следует, что системы Directum, DocsVision, Optima-Workflow и ЕВФРАТ-

Документооборот позволяют обеспечить необходимый уровень надёжности и безопасности СЭДО. В случае создания распределенной СЭДО количество одновременно работающих пользователей может измеряться тысячами. Хочется отметить, что системы Босс-Референт и CompaqMedia, реализованные на платформе Lotus Notes/Domino, предлагают наиболее развитые средства администрирования при распределенной работе за счет возможностей платформы.

Таблица 8 – Надёжность, безопасность

Система/Возможность	Б-Р	ГД	Д	Е-Д	СМ	D	DIS	DV	LD	O-W
Авторизация пользователей с паролем	+	+	+	+	+	+	+	+	+	+
Шифрование документов	+/-	-	+/-	+	+/-	+	+	+	+/-	+
Поддержка ЭЦП	+/-	+	+/-	+	+/-	+	+	+	+/-	+
Резервное копирование БД	+	-	+	+	+	+	-	+	+	+
Протокол событий	+	+/-	+	+	+	+	+	+	+	+

Контрольные вопросы для защиты работы:

- перечислить основные функции защиты информации современных СЭД;
- порядок реализации разграничения прав доступа в рамках СЭД;
- порядок реализации функции протоколирование событий в СЭД;
- порядок реализации функции поддержки электронной цифровой подписи;
- порядок реализации функции шифрования в СЭД;
- достоинства и недостатки российских и зарубежных СЭД по вопросам защиты информации;
- основные угрозы информации, обрабатываемой с СЭД;
- порядок организации внедрения СЭД на предприятии.

3.1.3 Оценка риска информационной безопасности СЭД.

Вопросы, подлежащие изучению:

- выбор организации и её структуры;
- анализ актуальных угроз для СЭД;
- определение вероятности реализации угроз.

Краткие сведения из теории

Назначение методики

Настоящая методика предназначена для проведения оценки рисков информационной безопасности (ИБ) в рамках построения или совершенствования системы информационной безопасности на предприятиях малого и среднего бизнеса.

Настоящая методика рекомендована для применения путем прямого использования устанавливаемых в ней положений при проведении оценки рисков ИБ и использовании результатов оценки рисков ИБ.

Постановка задачи

Основная задача данной методики заключается в том, чтобы определить численный показатель риска ИБ с целью принятия эффективных мер по защите информации. Предлагаемая методика оценки рисков позволяет выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

Обобщенный алгоритм проведения оценки рисков ИБ на предприятиях малого и среднего бизнеса (далее МСБ) приведен на рисунке 1.

Этапы	Название этапов
Этап 1	Идентификация активов
Этап 2	Определение риска несоответствия требованиям законодательства
Этап 3	Разработка модели угроз
Этап 4	Количественное определение риска
Этап 5	Определение допустимого уровня риска

Рисунок 1– Алгоритм оценки риска ИБ

Процедуры оценки рисков ИБ как комплексного подхода выполняются сотрудниками предприятия совместно с руководящим звеном, а также с сотрудниками отделов предприятия.

Этап 1. Идентификация активов. На данном этапе эксперты проводят интервью с персоналом каждого подразделения или отдела с целью выявления используемых активов. Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую вкладывает средства и которые, соответственно, требуют защиты со стороны предприятия. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение. Описание информационных активов проводится путём построения бинарных высказываний (описывалась в более ранних статьях) Могут существовать следующие типы активов:

1. Информация/данные (например, файлы, содержащие информацию о платежах или продукте).
2. Аппаратные средства (например, компьютеры, принтеры).
3. Программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения).
4. Оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели).
5. Программно-аппаратные средства (например, электронные носители информации).
6. Документы (например, контракты).
7. Продукция предприятия.
8. Услуги (например, информационные, вычислительные услуги).
9. Конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей).
10. Оборудование, обеспечивающее необходимые условия работы.
11. Персонал организации.
12. Престиж (имидж) организации.

Этап 2. Определение риска несоответствия требований законодательства в области ИБ. Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ МСБ. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0».

Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются.

В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ, который определяется по таблице 1.

Таблица 1- Уровень риска несоответствия требований по ИБ

Сумма выполненных требований	Риск несоответствия требованиям законодательства (R_n)
40–51	0,01
27–39	0,25
Менее 26	0,5
Не выполняются	0,9

Этап 3. Разработка модели угроз.

В методике с целью максимально точного определения риска ИБ необходимо разработать частную модель угроз ИБ предприятию. В модели угроз предлагается использовать уже разработанный и описанный в более ранних статьях метод оценки угроз с использованием алгоритма логического вывода Сорит. Определение вероятности наступления неблагоприятных событий определяется экспертом или группой экспертов, занимающихся разработкой модели угроз. Экспертным методом определяется и актуальность угроз ИБ.

После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или групп активов, подверженных этим угрозам, а также определяют вероятность реализации угроз. Весь процесс составления перечня актуальных угроз проводится с

использованием теории графов, с помощью которой описывается методика актуализации угроз.

Этап 4. Процедура количественной оценки рисков ИБ. Основным этапом в процессе оценки рисков является процедура количественного определения рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен в таблице 2.

Таблица 2 - Алгоритм количественного определения риска ИБ

Этапы	Название этапов
Этап 1	Анализ предприятия (структура и деятельность)
Этап 2	Идентификация активов (перечень сведений являющихся ценными для предприятия)
Этап 3	Определение риска несоответствия требованиям законодательства
Этап 4	Разработка модели угроз
Этап 5	Определение вероятности реализации угроз
Этап 6	Определение ценности информационных активов
Этап 7	Определение возможностей использования организационных и технических уязвимостей
Этап 8	Количественное определение риска
Этап 9	Определение допустимого уровня риска

Контрольные вопросы для защиты работы:

- сущность методики количественной оценки риска ИБ СЭД;
- защита отчёта по индивидуальному заданию.

3.1.4 Электронная цифровая подпись в системе электронного делопроизводства.

Вопросы, подлежащие изучению

- понятие электронной цифровой подписи;
- разновидности электронной цифровой подписи;
- порядок применения электронной цифровой подписи.

Краткие сведения из теории

Понятие электронной подписи (ЭП).

ЭП – формализованный и структурированный электронный документ, предназначенный для защиты подписанной информации от подделки, содержащий в себе полученный в результате криптографического преобразования информации с использованием закрытого ключа реквизит и позволяющий идентифицировать владельца сертификата, установить отсутствие искажения информации и обеспечивает неотказуемость подписавшегося.

ЭП – мощное средство контроля подлинности информации в электронном виде, обеспечения целостности электронных данных, подтверждения их авторства и актуальности. ЭП – это информационный объект, создаваемый для подписываемых данных, позволяющий удостовериться в целостности и аутентичности этих данных.

ЭП – это очень надежный инструмент, который позволяет, как установить авторство, так и подтвердить целостность любых данных в электронном виде. Например, полученное вами от, казалось бы, знакомого человека, письмо без электронной подписи может оказаться на самом деле поддельным или содержать искаженную после его отправления информацию. Использование электронной подписи такую возможность исключает. При проверке электронной подписи будет установлено, что документ был изменен после его подписания.

Распространенное мнение об электронной подписи – «это что-то криптографическое» - верно лишь отчасти. ЭП – это формализованная структура, электронный документ, состоящий из набора обязательных и не обязательных реквизитов – атрибутов электронной подписи. В состав обязательных атрибутов как раз и входит криптографическая часть, обеспечивающая надёжную идентификацию подписываемых данных и гарантирует надёжность источника информации о подписавшем.

Кроме криптографической части, ЭП обязательно содержит минимальную информацию о подписавшем и некоторую техническую информацию. Для прикладного использования, ЭП может содержать дату и время подписания, сведения для дополнительных механизмов проверки подписи, расширенную информацию о подписавшем, его полномочия и отношение к подписываемым данным, комментарии, файлы, графическое изображение собственноручной подписи и другие, функционально востребованные, данные.

ЭП поможет убедиться в том, что после подписи документа конкретным человеком никто «незаметно» этот документ не изменит, проверит надёжность отправителя электронного письма и сохранность его содержания, однозначно определит автора статьи, опубликованной в сети Интернет, и укажет дату публикации. Подробнее в разделе «Термины криптографии»

Если использовать электронную подпись при помощи «КАРМА», то можно заверять электронный документ и настоящей собственноручной подписью – при этом такая подпись будет надежно защищена от подделок, а выглядеть будет так, как на привычном бумажном документе.

Существуют различные виды электронной подписи.

Электронные подписи могут быть:

- присоединены к подписываемым данным;
- отсоединены от них;
- или находиться внутри данных.

Наиболее часто применяют электронные подписи к данным, хранящимся в файлах, а сама подпись относится ко всему содержимому файла.

Присоединенная ЭП

В случае создания присоединенной подписи создается новый файл электронной подписи, в который помещаются данные подписываемого файла. Этот процесс аналогичен помещению документа в конверт и его опечатыванию. Перед извлечением документа следует убедиться в сохранности печати (для электронной подписи в ее правильности). К достоинствам присоединенной подписи следует отнести простоту дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле. Этот файл можно копировать, пересылать и т.п. К недостаткам следует отнести то, что без использования средств СКЗИ уже нельзя прочесть и использовать содержимое файла, точно так же, как нельзя извлечь содержимое конверта, не расклеив его.

Отсоединенная ЭП

При создании отсоединенной подписи файл подписи создается отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется. Достоинством отсоединенной подписи является то, что подписанный файл можно читать, не прибегая к СКЗИ. Только для проверки подписи нужно будет использовать и файл с электронной подписью, и подписанный ей файл. Недостаток отсоединенной подписи - необходимость хранения подписанной информации в виде нескольких файлов (подписанного файла и одного или нескольких файлов с подписями). Последнее обстоятельство существенно осложняет применение подписи, так как при любых манипуляциях с подписанными данными требуется копировать и передавать несколько независимых файлов.

ЭП внутри данных

Применение электронной подписи этого вида существенно зависит от приложения, которое их использует, например электронная подпись внутри документа Microsoft Word или Acrobat Reader. Вне приложения, создавшего электронную подпись, без знания структуры его данных проверить подлинность частей данных, подписанных электронной подписью затруднительно.

«КАРМА» обеспечивает возможность создания и работы с присоединенной и отсоединенной подписями.

В электронной подписи содержится не только математический аналог подписи, позволяющий проверить целостность данных и гарантирующий их надежность. Кроме этого, ЭЦП содержит определенную информацию о подписавшем, времени подписи, сертификате подписавшего и другие реквизиты.

Разумеется, пользователь электронной подписи может не разбираться в таких тонкостях – именно для этого нужна «КАРМА». «КАРМА» не только возьмет на себя решение всех сложных технических проблем, но и предоставит Вам массу новых возможностей по защите информации

Порядок применения ЭП.

ЭП может применяться в разных областях:

ЭП может быть использована как ответственная подпись на электронном документе – то есть в качестве аналога собственноручной подписи и/или печати на бумажном документе. В частности, в этой ипостаси ЭП используется в системах электронного документооборота разного назначения.

Точно также ЭП широко используется для подписи программ или отдельных модулей, чтобы пользователь компьютера, загружая эти программы из Интернета, и используя их в работе, мог быть убежден в надежности и корректности их работы и надежности источника получения этих программ.

При ведении деловой переписки канцеляриями или секретарями разных компаний ЭП может служить в качестве «конверта» - на одном конце письмо запечатывают с помощью электронной подписи, а на финише получатель «вскрывает» конверт, предварительно убедившись в полной неприкосновенности и подлинности данных.

С помощью электронной подписи можно согласовывать электронные варианты документов (например, договоров) как между различными службами внутри одной организации, так и между различными организациями. В таком случае текст договора будет защищен от несогласованных изменений, а каждая ответственная инстанция должна будет согласовать документ с помощью собственной электронной подписи, подтвердив тем самым свое отношение к нему. Такая подпись безошибочно расскажет не только о том, кто подписал документ, но и укажет дату и время подписи. Если же сотрудник решит отказаться от ответственности за визирование документа или отправку информации в письме, скрепленном его электронной подписью, то ЭП легко его уличит. Например, часто договор требуется согласовать с юридическим отделом, бухгалтерией и другими подразделениями компании, и лишь после этого его

подпишут руководители обеих сторон. Такое согласование и визирование всеми ответственными службами можно проводить уже сейчас в электронном виде, применяя электронную подпись.

Система «КАРМА» расширяет и облегчает применение электронной подписи. Система позволит подписать электронный документ собственноручной подписью и даже поставить печать. И тогда документ будет не только скреплен «невидимой» человеку электронной подписью, но и «живой» подписью, введенной при помощи сенсорного экрана планшетного устройства или факсимиле. Также «КАРМА» может «наклеивать» на электронный документ так называемые «стикеры». Не создавая примечаний в самом документе, «стикер» позволит высказать свое отношение к нему, нанести резолюцию, выдать поручение и т.д. При этом каждый «стикер» будет привязан к содержанию документа – и если кто-то попытается изменить документ или «стикер», это будет обнаружено при просмотре стикера.

Контрольные вопросы для защиты работы

- дать определение электронной цифровой подписи;
- перечислить разновидности электронной цифровой подписи;

3.1.5 Модули и основные функции системы электронного делопроизводства «Дело»

Вопросы подлежащие изучению

- назначение системы «Дело»;
- основные понятия системы «Дело»;
- модули системы «Дело».

Краткие сведения из теории

Назначение системы «Дело»

Система автоматизации делопроизводства и электронного документооборота "ДЕЛО" (система "ДЕЛО") – программная система, предназначенная для автоматизации делопроизводства в организациях. Система функционирует на локальной вычислительной сети, объединяющей компьютеры, установленные на рабочих местах работников структурных подразделений, участвующих в технологических процессах делопроизводства.

Система позволяет обеспечить автоматизацию делопроизводства в службе документационного обеспечения управления (далее – ДОУ) и ее подразделениях: экспедиции, канцелярии, общем отделе, группе контроля и т.п., а также обеспечить автоматизацию делопроизводства в других структурных подразделениях.

К числу основных функций "русского" делопроизводства, требующих автоматизации, относятся следующие:

- регистрация всей поступающей корреспонденции, включая письма и обращения граждан, с последующим направлением корреспонденции на рассмотрение руководству организации или в ее структурные подразделения;
- регистрация всей исходящей корреспонденции организации и ее внутренних документов;
- организация работы с проектами документов, включая согласование (визирование) проекта документа, подписание (утверждение) проекта документа и регистрацию документа, созданного на основе проекта;
- организация движения документов (документооборота) внутри организации;
- осуществление контроля за своевременным и качественным исполнением поручений (документов);
- списание документов в дело в соответствии с принятой в организации номенклатурой дел;
- поиск документов по различным критериям и получение статистических отчетов по организации работы с документами.

При автоматизации документооборота организации система "ДЕЛО" может использоваться в двух целях.

Во-первых, система может сопровождать традиционно принятый в организации документооборот, упорядочивая технологию делопроизводства и облегчая рутинные операции по обработке документов. При этом система обеспечивает регистрацию входящих, исходящих и внутренних документов, контроль за исполнением поручений (резолюций) руководства, ввод отчетов исполнителей по поручениям (документам), организацию и учет движения документов между подразделениями и должностными лицами, включая движение бумажных оригиналов и копий документов. По каждому зарегистрированному документу в системе хранятся сведения, описывающие сам документ и весь процесс работы с ним в подразделениях: от регистрации до списания в дело, включая ход исполнения документа и рассылку во внешние организации.

По массиву всех зарегистрированных документов возможно проведение поисковых операций с целью отбора требуемых документов, в том числе, с целью контроля за исполнением поручений (документов).

Во-вторых, система позволяет существенно расширить рамки традиционной организации

документооборота за счет частичного или полного использования функций электронного документооборота и обработки документов на ЭВМ. Поэтому, система после ее внедрения в организации может служить своеобразным "мостом" для постепенного перехода от бумажной к безбумажной технологии обработки документов.

Модули СЭД «Дело»

При работе с системой "ДЕЛО" различным категориям пользователей необходим доступ к определенному набору функций системы. Например, работа системного технолога сводится к настройке системы, что обуславливает необходимость доступа к функциям, поддерживающим ввод значений в системные справочники и их редактирование. Круг задач других пользователей может определяться должностными инструкциями и быть ограниченным, например, только регистрацией поступающих документов или подготовкой отчетов руководству.

В связи с этим система "ДЕЛО" имеет модульную структуру, а каждый из модулей реализует набор функций, поддерживающих определенный технологический этап работы с документами.

Каждый модуль оформлен как отдельное Windows-приложение. Система "ДЕЛО" состоит из следующих модулей:

- *Документы;*
- *Отчетные формы;*
- *Справочники;*
- *Пользователи.*

При запуске того или иного модуля запрашивается идентификатор и пароль пользователя и проверяется наличие прав этого пользователя на работу с данным модулем.

Системный технолог работает со следующими модулями:

Модуль "*Пользователи*". Данный модуль предназначен для регистрации в системе новых пользователей, а также для установки прав доступа этих пользователей к другим модулям, картотекам, кабинетам и документам, хранящимся в системе "ДЕЛО";

Модуль "*Справочники*". Этот модуль используется для настройки системы "ДЕЛО" на структуру организации и технологию работы с документами путем ввода и редактирования содержимого справочников системы.

Модули, перечисленные ниже, предназначены для работы пользователей, непосредственно выполняющих те или иные делопроизводственные операции.

Модуль "*Отчеты*". Данный модуль обеспечивает формирование печатных отчетов, содержащих сведения о документообороте, сводок об исполнении документов и справок-напоминаний об исполнении документов.

Контрольные вопросы для защиты работы

3.1.6 Порядок выбора системы электронного документооборота

Вопросы, подлежащие изучению:

- алгоритм работы по выбору системы защищенного электронного документооборота;
- анализ организации и определение требований к будущей СЭД;
- сравнительный анализ СЭД.

Краткие сведения из теории

Алгоритм работы по выбору системы защищенного электронного документооборота

После того, как руководство организации приняло решение о переходе на электронный документооборот, наступает этап выбора и внедрения СЭЗДО.

Целесообразно проводить данную работу по алгоритму, представленному на рисунке.

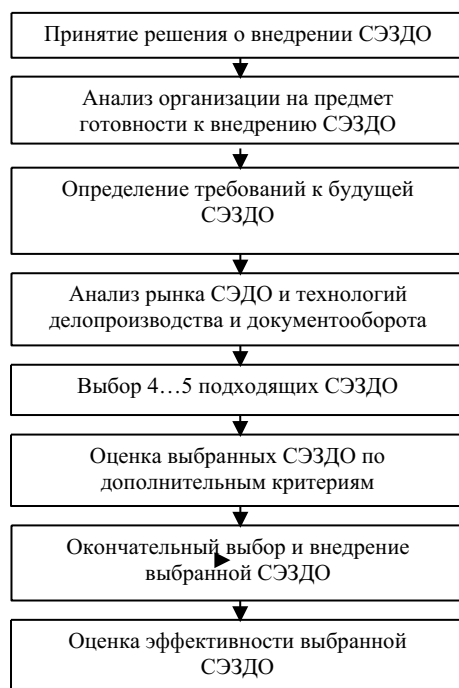


Рисунок – Алгоритм выбора системы электронного защищённого документооборота

Анализ организации и определение требований к будущей СЭД

Когда мы говорим о выборе (и последующем внедрении) какого либо ИТ-решения, нам, несомненно, следует учитывать особенности организации, в которой оно будет использоваться. Такими особенностями могут быть:

- размер предприятия (количество сотрудников не менее 50 человек);
- перспективы роста;
- наличие территориально удалённых офисов;
- зрелость ИТ- инфраструктуры и подготовка сотрудников;
- наличие других информационных систем;
- объём хранимой конфиденциальной информации, степень её конфиденциальности и скорость пополнения;
- длительность и надёжность хранения информации;
- наличие финансовых ресурсов;
- личные цели участников проекта внедрения и др.

Определение требований к будущей системе электронного защищённого документооборота

Такими требованиями могут быть:

- обеспечение эффективного управления и прозрачности деятельности организации на всех уровнях;
- уровень защищённости информации;
- накопление информации, управление данными и регламентирование доступа;
- формализация деятельности каждого сотрудника;
- сокращение оборота бумажных документов. Экономия ресурсов за счёт сокращения расходов на управление бумажными потоками в организации;
- снижение стоимости хранения бумажных документов, облегчение их поиска;
- поддержка системы контроля качества;
- формализация и обеспечение соответствующего инструментария для последующей оптимизация бизнес-процессов организации

Контрольные вопросы для защиты работы

- сущность алгоритма работы по выбору системы защищённого электронного документооборота;
- сущность анализ организации и определение требований к будущей СЭД;
- сущность порядка применения электронной цифровой подписи.

3.1.7 Работа с модулями СЭД «Дело»

Вопросы, подлежащие изучению:

- заполнение базовых справочников;
- регистрация пользователей;
- заполнение дополнительных справочников;
- работа со справочником «Подразделение»
- работа со справочником «Кабинеты»;
- работа со справочником «Группы документов»;
- работа с внутренними документами
- работа с исходящими документами;
- заполнение регистрационных карточек;
- анализ результатов работы.

Краткие сведения из теории

Работа в модуле Документы

Модуль "Документы". Этот модуль реализует основные функциональные возможности системы "ДЕЛО". (Окно модуля "Документы" см. на Рисунке 1).

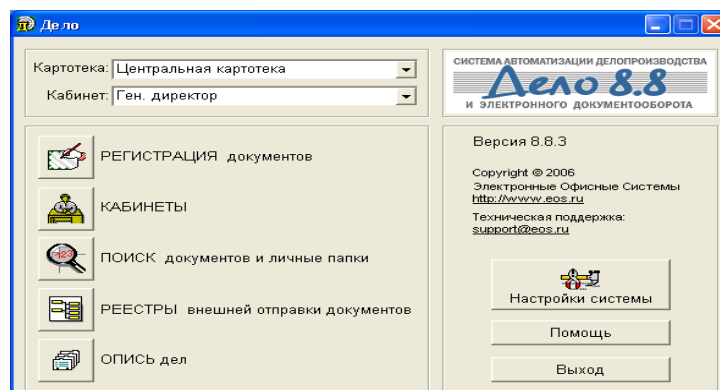


Рисунок 1 - Окно модуля Документы

На главном окне модуля "Документы" (См. Рисунок 12) содержатся кнопки, открывающие доступ к следующим функциям системы:

Регистрация документов – данная функция обеспечивает регистрацию документов в системе, т.е. присвоение документу регистрационного номера, создание и заполнение для него РК и направление документа на исполнение;

Кабинеты – эта функция предоставляет доступ к содержимому папок кабинета с целью исполнения документов, включая выдачу поручений по документу, оформление отчетов исполнителей, контроль исполнения, снятие документа с контроля, списание документа в дело и т.д. Кроме того, данная функция используется для работы с проектами документов (создание проектов, визирование и подписание проектов документов);

Поиск документов и личные папки – эта функция предназначена для поиска документов и проектов документов по задаваемым пользователем критериям отбора. Для хранения результатов поиска пользователь может создавать личные папки и помещать в них отобранные документы (проекты документов);

Реестры внешней отправки документов – данная функция используется для формирования реестров внешней рассылки документов для их отправки по адресатам;

Опись дел – данная функция обеспечивает просмотр документов, списанных в дела, и их закрытие. Кроме того, эта функция используется для выгрузки информации о делах в БД подсистемы "Архивное дело".

Доступ пользователей к тем или иным модулям, а также права, необходимые для выполнения каких-либо функций в этих модулях, устанавливаются системным технологом.

Для того чтобы документ был учтен в системе, он должен быть зарегистрирован. При регистрации формируется РК документа, в которую заносятся сведения о документе, и присваивается регистрационный номер, формируемый по единым для данной подгруппы документов правилам.

Регистрируются как поступившие извне, так и созданные внутри организации документы: письма, приказы, договоры, акты и прочее.

Регистрация документов может производиться централизованно (в одном подразделении) или децентрализованно.

РК содержит полный набор реквизитов, предусмотренных Типовой инструкции по

делопроизводству в федеральных органах исполнительной власти, утвержденной приказом Минкультуры России от 08 ноября 2005 г. № 536. Для отражения ведомственной или отраслевой специфики состав полей РК может быть расширен за счет дополнительных реквизитов. Новые реквизиты могут создаваться системных технологом самостоятельно.

К РК документа могут прикрепляться файлы документов любого формата.

Некоторые поля РК заполняются путем выбора значений из справочников, а в остальные поля информация вводится с клавиатуры. При этом в системе "ДЕЛО" существует возможность выполнять проверку орфографии текста, введенного с клавиатуры. Кроме этого каждый пользователь может вести список стандартных текстов, используемых для экономии времени при заполнении полей, информация в которые вводится с клавиатуры.

Файлы исходящих и внутренних документов по стандартной технологии могут быть прикреплены к РК. Для документов, которые готовятся в MS Word, реализована упрощенная процедура регистрации прямо из среды текстового процессора.

Документы в системе регистрируются однократно. После осуществления регистрации РК может быть переслана в кабинеты должностных лиц, которые должны осуществлять работу с документом или должны быть с ним ознакомлены. Также, при необходимости, на основании документа может быть издано поручение, в этом случае РК документа вместе с информацией о поручении автоматически направляется в кабинеты исполнителей и контролера.

Таблица 3 - Реквизиты РК, имеющей вид "Входящие"

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
1.	Регистрационный номер документа		Номер (индекс) документа, задаваемый по принятым в организации правилам
2.	Дата регистрации		Дата регистрации поступившего в организацию документа
3.	Экземпляр		Номер(а) экземпляра документа
4.	Гриф доступа		Гриф доступа пользователей к содержимому карточки по принятой в организации классификации
5.	Плановая дата исполнения		Плановая дата исполнения документа
6.	Фактическая дата исполнения		Фактическая дата исполнения документа
7.	Состав		Количественные характеристики состава документа. Количество листов, наличие и количество приложений и т.п.
8.	Корреспонденты	Наименования организаций; Исходящие номера;	Информация об авторах документа и их регистрационных реквизитах документа

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
		Исходящие даты; Кто подписал; Примечание	
9.	Доставка		Наименование способа получения документа по принятой в организации классификации
10.	Почтовый номер		Реквизит доставки документа (номер заказного письма, телеграммы и т.п.)
11.	Кому адресован	Наименования подразделений или ФИО и должности работников	Адресаты документа в организации
12.	Сопроводительные документы	Содержание; Корреспонденты; Исходящие номера; Исходящие даты; Кто подписал; Состав документа; Примечание	Описание характеристик сопроводительного документа и его авторов
13.	Адресаты	Для организаций указываются: Наименование организации; Дата, время и вид отправки; Состав документа; Кому адресован документ; регион, город, почтовый индекс, адрес; e-mail; Полное название организации.	Перечень адресатов документа (организации, граждане, внутренние адресаты организации) и атрибуты отправки им документа
14.	Журнал передачи документа	Дата и время передачи документа; Вид документа (оригинал, копия); Номер экземпляра; Наименования подразделений или ФИО работников, которым передан документ;	Информация о движении бумажного документа
15.	Краткое содержание		Краткое описание содержания документа
16.	Рубрики	Наименования рубрик; Коды рубрик	Тематические рубрики, по которым классифицируется документ. Могут быть расширены дополнительными реквизитами
17.	Связки	Типы связок; Номера связанных документов	Информация о связи текущего документа с другими документами (проектами документов)
18.	Файлы	Наименования файлов; Гриффы доступа	Описание прикрепленных файлов и гриффы доступа к ним
19.	Примечание		Поле для ввода произвольного текста комментария с характеристиками документа или, возможно, способа его обработки
20.	Дополнительные реквизиты		По усмотрению организации можно дополнить реквизитный состав РК

В-6/2007 от 22.01.2007 Обращения граждан

Файл Действия Реквизиты Поручения Вид

№: В-6/2007 От: 22/01/2007 Экз. №: 1 Доступ: общий План: 05/02/2007 Факт: 00/00/0000

Корреспонденты (1 из 1)

Гражд.: Валяевская Т.М. Город: Ставрополь

Регион: Южный федеральный округ Индекс: 111111 Ответ: ☐

Адрес: Прямая ул. д. 14

Состав: 2

Доставка: Почта

Почт. №:

Сопр. документ (0)

Адресаты (0)

Журнал передачи

Файлы

жалоба.jpg

Кому(1): Михайлов А.В. - Генеральный директор Коллективное ☐ Анонимное ☐

Содерж.: Жалоба на работу строительной компании "Надега"

Рубр.(0): Связки(0):

Прим.:

Поручение (0 из 0)

Автор: от 00/00/0000 План: 00/00/0000 Факт: 00/00/0000

Текст:

Центральный аппарат Центральный аппарат

Таблица 4 - Реквизиты РК, имеющей вид "Письма граждан"

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
1.	Регистрационный номер письма		Номер (индекс) документа, задаваемый по принятым в организации правилам
2.	Дата регистрации		Дата регистрации поступившего в организацию письма
3.	Экземпляр		Номер(а) экземпляра письма
4.	Гриф доступа		Гриф доступа пользователей к содержимому карточки по принятой в организации классификации
5.	Плановая дата исполнения		Плановая дата исполнения документа
6.	Фактическая дата исполнения		Фактическая дата исполнения документа
7.	Состав		Количественные характеристики состава документа. Количество листов, наличие и количество приложений и т.п.
8.	Корреспонденты	ФИО граждан; Регионы; Города проживания; Почтовые индексы и адреса авторов	Информация об авторах письма и их почтовые реквизиты
9.	Ответ		Признак того, что данному корреспонденту в дальнейшем будет отправлен ответ
10.	Признак коллективности		Признак коллектива авторов письма
11.	Признак анонимности		Признак анонимности письма
12.	Доставка		Наименование способа получения письма по принятой в организации классификации
13.	Почтовый номер		Реквизит доставки письма (номер заказного письма телеграммы и т.п.)
14.	Кому адресован	Наименования подразделений или ФИО и должности адресатов	Адресаты письма в организации
15.	Сопроводительные документы	Содержание; Корреспонденты; Исходящие номера;	Описание характеристик сопроводительного документа и его авторов

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
		Исходящие даты; Кто подписал; Состав документа; Примечание	
16.	Адресаты	Для организаций указываются: Наименование организации; Дата, время и вид отправки; Состав документа; Кому адресован документ; регион, город, почтовый индекс, адрес; e-mail; Полное название организации.	Перечень адресатов документа (организации, граждане, внутренние адресаты организации) и атрибуты отправки им документа
17.	Журнал передачи документа	Дата и время передачи документа; Вид документа (оригинал, копия)	Информация о движении бумажного документа
18.	Краткое содержание		Краткое описание содержания письма
19.	Рубрики	Наименования рубрик; Коды рубрик	Тематические рубрики, по которым классифицируется письмо. Могут быть расширены дополнительными реквизитами
20.	Связки	Типы связок; Номера связанных документов	Информация о связи письма с другими документами (проектами документов)
21.	Файлы	Наименования файла; Грифы доступа	Описание прикрепленных файлов и грифы доступа к ним
22.	Примечание		Поле для ввода произвольного текста комментария с характеристиками письма или, возможно, способа его обработки
23.	Дополнительные реквизиты		По усмотрению организации можно дополнить реквизитный состав РК

П-2 от 22.01.2007 Приказы по основной деятельности

Файл Действия Реквизиты Поручения Вид

№: П-2 От: 22/01/2007 Экз. №: 1 Доступ: общий План: 12/02/2007 Факт: 00/00/0000

Подп.(1): Михайлов А.В. - Генеральный директор

Содерж.: О проведении обучения

Исполк: Ломакин Р.А. - Нач. отдела кадров

Визы(9): Ломакин Р.А. - Нач. отдела кадров (21/01/2007)

Рубр.(0): Связки(0):

Прим.:

Адр.(0):

Состав: 2 + 4

Сописполнители (0)

Журнал передачи

Файлы

приказ.jpg

список обучающих

Поручение (1 из 1)

№ пункта: 1 План: 12/02/2007 Факт: 00/00/0000

Текст: Провести обучение в соответствии с графиком обучения и списком групп обучающихся

Королева И.В. - Вед

Центральный аппарат

Таблица 5 - Реквизиты РК, имеющей вид "Исходящие"

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
---	------------------------	---------------------------------------	----------

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
1.	Регистрационный номер документа		Номер (индекс) документа, задаваемый по принятым в организации правилам
2.	Дата регистрации		Дата подписания документа
3.	Экземпляр		Номер(а) экземпляра документа
4.	Гриф доступа		Гриф доступа пользователей к содержимому карточки по принятой в организации классификации
5.	Плановая дата исполнения		Плановая дата исполнения документа
6.	Фактическая дата исполнения		Фактическая дата исполнения документа
7.	Кто подписал	ФИО и должности работников; Дата и время подписания	Информация о должностных лицах, подписавших документ
8.	Состав		Количественные характеристики состава документа. Количество листов, наличие и количество приложений и т.п.
9.	Краткое содержание		Краткое текстовое описание содержания документа
10.	Исполнитель документа		Наименование подразделения или ФИО и должность работника организации, подготовившего документ
11.	Соисполнители	Наименования организаций; Исходящие номера; Исходящие даты; Кто подписал	Соисполнители совместного с другими организациями документа
12.	Журнал передачи документа	Дата и время передачи документа; Вид документа (оригинал, копия);	Информация о движении бумажного документа
13.	Визы	Кто визировал; Дата визирования; Примечание	ФИО и должности работников организации, визировавших документ
14.	Рубрики	Наименования рубрик; Коды рубрик	Тематические рубрики, по которым классифицируется документ. Могут быть расширены дополнительными реквизитами
15.	Связки	Типы связок; Номера связанных документов	Информация о связи текущего документа с другими документами (проектами документов)
16.	Файлы	Наименования файлов; Гриф доступа	Описание прикрепленных файлов и грифы доступа к ним
17.	Примечание		Поле для ввода произвольного текста с характеристиками документа или, возможно, способа его обработки
18.	Адресаты	Для организаций указываются: Наименование организации; Дата, время и вид отправки; Состав документа; Кому адресован документ; регион, город, почтовый индекс, адрес; e-mail;.	Перечень адресатов документа (организации, граждане и внутренние адресаты организации) и атрибуты отправки им документа
19.	Дополнительные реквизиты		По усмотрению организации можно дополнить реквизитный состав РК

Работа над проектами документов

В системе "ДЕЛЮ" реализовано понятие "проектов документов" и поддержан полный цикл работы с проектами:

- создание РКПД, в том числе и "во исполнение" документа;

- изменение проекта с хранением предыдущих версий;
- согласование (визирование) проекта документа;
- утверждение (подписание) проекта документа;
- регистрация документа, созданного на основе проекта.

Для работы с проектами используется специальный тип карточки – РКПД (См. Рисунок 16), включающей перечень должностных лиц, визирующих и подписывающих проект, и маршрут визирования.

Исполнитель (разработчик) проекта документа может анализировать ход визирования и подписания проекта.

Должностные лица, которым документ направлен на визирование, могут завизировать его, высказать свои замечания и/или оформить замечания в виде отдельного файла.

В процессе визирования (подписания), визирующие и подписывающие должностные лица, при необходимости, могут добавить дополнительных визирующих должностных лиц.

Системой поддерживается версионность проектов документов. На любой стадии согласования проекта можно приостановить работу с текущим вариантом и на основе замечаний к нему создать новый. История работы с вариантами проекта документа может быть сохранена.

При регистрации согласованного и подписанного проекта как внутреннего или исходящего его РК автоматически создается на основе РКПД.

ФИО	Виза / подпись	Дата	Направлено	Срок
В Ломакин Р.А. - Нач. отдела к		22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41
В Ковалевский С.Ю. - Начальн	Согласен	22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41
В Аведокатов П.Б. - Нач. отдела		22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41
В Добронравов А.Г. - Начальн		22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41
В Плахов А.В. - Управляющий	Согласен	22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41
В Киселев - Руководитель отде		22/01/2007 11:17:00	22/01/2007 11:18:41	24/01/2007 11:18:41

Таблица 6 - Реквизиты РКПД

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
1.	Регистрационный номер		Номер (индекс) проекта документа, задаваемый по принятым в организации правилам
2.	Дата регистрации		Дата создания и регистрации проекта документа
3.	Плановая дата		Дата, к которой проект документа должен пройти все необходимые стадии подготовки проекта и стать подписанным документом
4.	Гриф доступа		Гриф доступа пользователей к содержимому регистрационной карточки, которая будет создана на основе данного проекта, по принятой в организации классификации
5.	Исполнитель		ФИО и должность работника организации, подготовившего проект документа
6.	Состав		Количественные характеристики состава проекта документа. Количество листов, наличие и количество приложений и т.п.
7.	Краткое содержание		Краткое текстовое описание содержания проекта документа
8.	Версия		Номер текущей версии проекта документа
9.	Связки	Типы связей; Номера связанных документов	Информация о связи текущего проекта документа с другими документами (проектами документов)

№	Наименование реквизита	Состав (для множественных реквизитов)	Описание
10.	Примечание		Поле для ввода произвольного текста с характеристиками проекта документа или, возможно, способа его обработки
11.	Адресаты	См. таблицу 5	Перечень адресатов проекта документа (организации, граждане и внутренние адресаты организации) и атрибуты отправки им проекта документа
12.	Файлы	Наименования файлов; Гриффы доступа	Описание прикрепленных файлов и гриффы доступа к ним
13.	Визы и подписи		Информация о ходе согласования и утверждения проекта документа (ФИО и должности визирующих и подписывающих должностных лиц, содержание визы/подписи, дата и время отправки проекта документа на визирование/подписание, срок выполнения визирования/подписания, даты визирования /подписания, ФИО работника, направившего проект на визирование /подписание)

Контроль за исполнением поручений (документов)

Контроль за исполнением поручений (документов) – совокупность действий, целью которых является содействие своевременному и качественному исполнению поручений (документов), обеспечение получения аналитической информации, необходимой для оценки деятельности структурных подразделений, филиалов, конкретных сотрудников.

Данное словосочетание ("контроль за исполнением поручений") вошло в употребление в конце 2005 г. в связи с появлением Типовых регламентов федеральных органов власти. До этого времени использовался другой термин "контроль за исполнением документов".

Поручения могут содержаться в документах, а также в резолюциях руководителей по исполнению документов.

Система "ДЕЛО" с версии 8.8.0 ввела новое понятие "Поручение" и следующие виды поручений:

- резолюция;
- пункт;
- подчиненная резолюция;
- проект резолюции.

В отличие от *резолюции* (т.е. поручения, выдаваемого на основании документа), *пункт* – это поручение, содержащееся в тексте самого документа. Как по резолюциям, так и по пунктам, могут выноситься *подчиненные резолюции*, относящиеся не к документу в целом, а к его конкретному пункту или конкретной резолюции. Подчиненная резолюция, в свою очередь, может иметь свои подчиненные резолюции (более низкого уровня иерархии) и т.д. – такой подход позволяет повысить эффективность контроля исполнения поручений.

Вид поручения "*проект резолюции*" используется при подготовке помощником руководителя проекта резолюции руководства. В дальнейшем проект резолюции передается на утверждение руководителю, после чего рассылается исполнителям.

Документ считается контрольным, если на его основании создано хотя бы одно контрольное поручение, которое еще не снятое с контроля. Для контрольных документов, по которым заведено поручение, автоматически отслеживаются сроки исполнения, особо выделяются контролируемые документы и документы с истекшими сроками исполнения.

Система позволяет формировать напоминания исполнителям и сводки об исполнении контрольных документов.

Контролю подлежат все документы, имеющие контрольные поручения. Снятие с контроля происходит после проставления фактической даты исполнения поручения. Когда поручение снято с контроля, запись о нем (о РК документа, на который оно было заведено) автоматически удаляются из всех кабинетов.

При рассылке контрольных поручений (кроме сообщений в кабинетах исполнителей) создается сообщение в папке "На контроле" автора поручения и контролера. Контроль исполнения также может осуществляться путем поиска документов по реквизитам контрольных поручений.

Исполнение поручений (документов)

Информация о документах, направленных тем или иным должностным лицам на исполнение,

находится в папке *"Поступившие"* соответствующего кабинета. Прежде чем принять какой-либо документ к исполнению исполнитель должен удостовериться, что документ направлен к нему не по ошибке. Убедившись в этом, он принимает документ к исполнению, сообщение об этом документе или поручении при этом перемещается из папки *"Поступившие"* в папку *"На исполнении"*. После окончания работы над документом исполнитель находит РК этого документа, вводит текст отчета и, при необходимости, связывает РК исполняемого документа с РК одного или нескольких документов, на которые ссылается в своем отчете (например, в случае подготовки исполнителем исходящего или внутреннего документа). Если поручение было неконтрольным, то сообщение, связанное с этим поручением, удаляется из папки *"На исполнении"*, после ввода отчета об исполнении.

РК контрольного документа и сами контрольные поручения выделяются соответствующим признаком. Сообщения о контрольном поручении в кабинетах ее исполнителей и контролера остаются до тех пор, пока поручение не будет снято с контроля. В системе снятие поручения с контроля происходит, как правило, после получения итоговых отчетов от ответственных исполнителей; при этом указывается фактическая дата исполнения поручения и снимается признак контрольности.

После снятия поручения с контроля сообщения о нем автоматически удаляются из кабинетов ее исполнителей, контролера и автора.

Правила по исполнению поручений описаны в главе 12 "Руководства пользователя".

Организация документооборота

В системе существует несколько механизмов организации движения документов. Каждый механизм обеспечивает оптимальное выполнение того или иного делопроизводственного процесса:

- при работе над проектом документа карточка автоматически пересылается по последовательному или параллельному маршруту между заранее определенными согласующими или подписывающим (утверждающим) должностными лицами. В процессе пересылки проекта учитывается характер вынесенных виз, контролируются сроки рассмотрения;
- после заведения поручений документ автоматически пересылается исполнителям, контролеру и автору поручения, при этом контролируются сроки исполнения поручений;
- В системе реализовано также множество других механизмов движения документов: внутренняя адресация, пересылка электронных документов внешним организациям, полный контроль всех видов движения бумажных документов и прочие.

Отслеживание движения бумажного документа происходит с помощью *"Журнала передачи бумажных оригиналов и копий документов"*, в который заносится информация:

- о передаче бумажного оригинала или копии должностному лицу;
- о списании документа в дело;
- об уничтожении документа.

На основании данных, фиксируемых в *"Журнале передачи бумажных оригиналов и копий документов"*, при необходимости, можно формировать и печатать реестр документов для их последующей передачи под расписку.

Списание документов в дело

После исполнения документа он списывается в дело. Списание документа в дело осуществляется путем занесения в РК записи, содержащей наименование дела (согласно справочнику *"Номенклатура дел"*), дату и время списания. Справочник *"Номенклатура дел"* заполняется системным технологом в соответствии с ежегодно утверждаемой номенклатурой

Контрольные вопросы для защиты работы

1. Правила заполнения базовых справочников.
2. Порядок регистрации пользователей.
3. Порядок заполнения дополнительных справочников.
4. Порядок работы со справочником «Подразделение».
5. Порядок работы со справочником «Кабинеты».
6. Порядок работы со справочником «Группы документов».
7. Правила работы с внутренними документами.
8. Порядок работы с исходящими документами.
9. Правила заполнения регистрационных карточек.

3.1.8 Оценка эффективности систем электронного документооборота.

Вопросы, подлежащие изучению

- оценка эффективности и возврата инвестиций от внедрения системы электронного документооборота;
- порядок расчёта расходов и доходов от внедрения СЭД.

Краткие сведения из теории

Оценка эффективности и возврата инвестиций от внедрения системы электронного

документооборота.

Внедрение САДЭД – это здоровое решение в области бизнеса, а не технологий. Принятие руководством организации решения о вложении средств в улучшенную систему управления документацией даст практический результат – более качественный и оперативный сервис, более эффективное рабочее пространство и, что особенно важно, преимущество перед конкурентами.

Анализ соотношения цена/польза – это логическая процедура оценки соотношения плюсов (пользы) и минусов (цен) каждого из альтернативных вариантов. Плюсы и минусы можно определять с точки зрения подающихся или неподдающихся численной оценке – или осязаемых и неосязаемых – факторов.¹

Консервативный стиль обращения с документами в бумажном виде на фоне экспоненциально растущего общего объема в мире лишь увеличивает расходы на бумагу и расходные материалы, офисные площади вынужденно нерационально тратятся на хранение архивных дел, подшивок печатных изданий, распечатанной электронной корреспонденции.

⇒ На поиск, согласование и утверждение документов приходится 30% рабочего времени сотрудников. Это примерно 1 месяц в год;

⇒ На ожидание поступления документов – 20 %;

⇒ На передачу документов между подразделениями – 10 %;

⇒ На подготовку стандартных отчетов о движении документов – 10 %;

⇒ На создание новых документов тратится примерно 30% рабочего времени;

⇒ 20 - 30% поставленных задач вообще не решаются;

⇒ 6 - 15% бумажных документов безвозвратно теряется;

⇒ В среднем создается 19 копий каждого документа.

САДЭД не только поможет решить эти проблемы, но и принесет экономическую выгоду.

⇒ Увеличение скорости и точности поиска позволяет сэкономить от 2х до 5ти часов в неделю на одного сотрудника и составляет от 5-15%;

⇒ Применение систем электронного документооборота увеличивает производительность труда сотрудников на 20-50%, а время обработки одного документа уменьшается более чем, на 75, а уменьшение затраты на хранение на 80%;

⇒ Наличие прототипов и шаблонов документов позволяет экономить от 20-30% времени от трудозатрат на создание новых документов, а это около 7,5% от полного рабочего времени сотрудников.

⇒ Утверждение и согласование документа на одного сотрудника составит 10-30%;

⇒ И наконец, по оценкам специалистов внедривших СЭД, их использование может способствовать увеличению прибыли предприятия на 5-15%.

Таким, образом, средний процент экономии времени при использовании СЭД составляет более 60%.

Порядок расчёта расходов и доходов от внедрения СЭД.

Общая стоимость расходов определяется по следующей формуле:

$$P = \sum P_i,$$

где i - статьи расходов на внедрение системы.

Внедрение АС ДОУ на основе промышленной СУБД содержит следующие статьи расходов:

1. Стоимость покупаемых клиентских лицензий (P_L) к СУБД (Microsoft SQL, Oracle, Sybase и т. д.) на определенное количество рабочих мест.

2. Стоимость однопроцессорного варианта СУБД (P_6) с возможностью подключения неограниченного количества клиентских лицензий.

3. Стоимость обеспечения дополнительными программно-техническими средствами (P_n) установленного количества рабочих мест, дающих возможность осуществить поточное сканирование, внедрение ЭЦП и шифрования.

4. Стоимость работ по запуску системы (P_3) равна следующей величине:

$$P_3 = M * W + M * W * F(N),$$

где M - количество месяцев, необходимое для выполнения работ по запуску системы на N мест;

W - средняя стоимость 1 месяца работ ;

$F(N)$ - функция характеристики размера организации, позволяющей учесть в расходах усложнение задачи за счет величины размера организации. Поведение этой функции качественно похоже на логарифм от величины N и приблизительно равно следующим значениям: если $N=100$, то $F(N)=0,3$; если $N=200$, то $F(N)=0,35$, а если $N > 100$, то $F(N)=0,4$.

5. Стоимость обучения (P_o) пользователей, администраторов системы и персонала,

сопровождающего систему.

6. Стоимость годового сопровождения (P_c) компанией системы.

7. Стоимость конвертации (P_k) данных.

Таким образом, суммарные расходы по внедрению и эксплуатации АС документационного обеспечения управления за год будут равны

$$P_d = P_l + P_b + P_p + P_z + P_o + P_c * (12 - M) / 12 + P_k.$$

Расчет доходов

Расчет доходной части осуществляем исходя из того, что экономический эффект состоит только из стоимости сэкономленного рабочего времени сотрудников ($\mathcal{E}_{рв}$) и стоимости бумаги ($\mathcal{E}_{сб}$), сэкономленной при переходе на электронный документооборот

$$\mathcal{E} = \mathcal{E}_{рв} + \mathcal{E}_{сб}.$$

Расчет стоимости сэкономленного рабочего времени сотрудников выполняется на основе экспертных оценок.

Практически для любого документа в достаточно давно существующей организации всегда найдется прототип. Чаще всего прототип экономит от 20 до 30% времени от трудозатрат на создание документа. Если каждый сотрудник тратит на создание новых документов ($\mathcal{E}_{сд}$) примерно 30% своего рабочего времени, то общая экономия времени сотрудников при наличии прототипов составит около 7,5% от их полного рабочего времени.

Экономия времени на поиск документа ($\mathcal{E}_{пд}$) достаточно хорошо измерена и реально находится в диапазоне 5-10%.

Ускорение бизнес-процессов наиболее тяжело поддается априорной оценке. При бумажном документообороте процесс согласования и утверждения документа ($\mathcal{E}_{уд}$) длителен и невозможен контроль задержки исполнения. При внедрении автоматизированной системы документационного обеспечения управления документы передаются на следующую инстанцию сразу же после исполнения. Таким образом, многостадийное утверждение и согласование может быть сокращено в несколько раз. В этом случае экспертная оценка экономии на одного сотрудника составит 10-30% рабочего времени.

Экономия трудозатрат ($\mathcal{E}_t$), по нашим предположениям, составит величину

$$\mathcal{E}_t = \mathcal{E}_{сд} + \mathcal{E}_{пд} + \mathcal{E}_{уд}.$$

Среднемесячные расходы в организации на одного сотрудника (S).

Тогда экономия рабочего времени ($\mathcal{E}_{рв}$) сотрудников за год составит

$$\mathcal{E}_{рв} = \mathcal{E}_t * 12 * N * 8 = (\mathcal{E}_{сд} + \mathcal{E}_{пд} + \mathcal{E}_{уд}) * 12 * N * S.$$

Мощность документопотока определяется через показатели объема документов за единицу времени (год, месяц) [25]:

$$V = \sum D_{ij}, \text{ где } V - \text{объем документации за единицу времени;}$$

D_{ij} - количество документов в j -й группе по i -му структурному подразделению.

В течение года работники машбюро организации *распечатали* ($\mathcal{E}_m$) *страниц текста*, а работники архива *сделали* ($\mathcal{E}_a$) *листов копий подлинников документов*. Ежегодно организация осуществляет отправку принимаемых актов по полной или обязательной рассылке. За год было *разослано* ($\mathcal{E}_p$) *единиц корреспонденции* (листов формата А4).

Стоимость сэкономленной бумаги ($\mathcal{E}_{сб}$) (без учета нанесения информации) исходя из того, что одна пачка (500 листов) стоит C , составит

$$\mathcal{E}_{сб} = (\mathcal{E}_m + \mathcal{E}_a + \mathcal{E}_p) / 500 * C. \text{ Общая экономия равна } \mathcal{E} = \mathcal{E}_{рв} + \mathcal{E}_{сб} = (\mathcal{E}_{сд} + \mathcal{E}_{пд} + \mathcal{E}_{уд}) * 12 * N * S + (\mathcal{E}_m + \mathcal{E}_a + \mathcal{E}_p) / 500 * C.$$

Расчетный срок окупаемости автоматизированной системы документационного обеспечения управления на основе промышленной СУБД равен

$$T = P_d / \mathcal{E} = [P_l + P_p + P_z + P_o + P_c * (12 - M) / 12 + P_b + P_k] / [(\mathcal{E}_{сд} + \mathcal{E}_{пд} + \mathcal{E}_{уд}) * 12 * N * 8 + (\mathcal{E}_m + \mathcal{E}_a + \mathcal{E}_p) / 500 * C].^2$$

Контрольные вопросы для защиты работы

- сущность оценки эффективности и возврата инвестиций от внедрения системы электронного документооборота;
- порядок расчёта расходов и доходов от внедрения СЭД.

4. Перечень рекомендуемой литературы

4.1 Основная литература

1. Карусевич, Т. Е. Организация электронного документооборота в системах управления ресурсами и взаимоотношениями предприятия : учебное пособие / Т. Е. Карусевич, К. А. Потапова. — Москва : РТУ МИРЭА, 2021. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/226550>
2. Анацкая, А. Г. Защита электронного документооборота : учебное пособие / А. Г. Анацкая. — Омск : СибАДИ, 2019. — 87 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/149493> Учебное издание

4.2 Дополнительная литература

1. Смирнова, Г.Н. Электронные системы управления документооборотом. Учебное пособие, практикум по дисциплине [Электронный ресурс] / Г.Н. Смирнова. - М. : Московский государственный университет экономики, статистики и информатики, 2004. - 115 с. - ISBN 5-7764-0399-- URL: <http://biblioclub.ru/index.php?page=book&id=90954>
2. Некраха А.В., Шевцова Г.А. Организация конфиденциального делопроизводства. – М.: Академический проект, 2010. – 224 с.
3. Бутакова А.В., Семененко В.П. Защита и обработка конфиденциальных документов. – М.: Московский технологический институт, 2009. – 238 с.
4. Корнеев И. К., Степанов Е. А. Защита информации в офисе. – М.: Проспект, 2009. – 336 с.
5. Кудряев В.А. Организация работы с документами. – М.: ИФРА, 2009. – 278 с.

Методы и средства защиты информации в системах электронного документооборота

Редактор М.И. Толмачев
Технический редактор, компьютерная верстка А.Х. Ардеев

Подписано в печать 03.05.2013

Формат 60 84 1/16

Усл. печ. л. 0,7

Уч.- изд. 0,8

Бумага газетная

Тираж 30 экз.

Заказ 36

Отпечатано в Издательско-полиграфическом комплексе
СКФУ
355009, Ставрополь, ул. Кулакова 2а.