Колледж связи 54

Комплексная защита информации

Сущность и задачи КЗИ

Комплексная защита информации **(КЗИ)** – совокупность людей, процедур и оборудования, защищающих информацию от несанкционированного доступа, модификации либо отказа доступа

ЗАДАЧИ КЗИ:

1. Регламентация действий пользователей;
2. Установление юридической ответственности за выполнение правил ИБ;
3. Явный и скрытый контроль за порядком информационного обмена;

Задачи Комплексной защиты информации

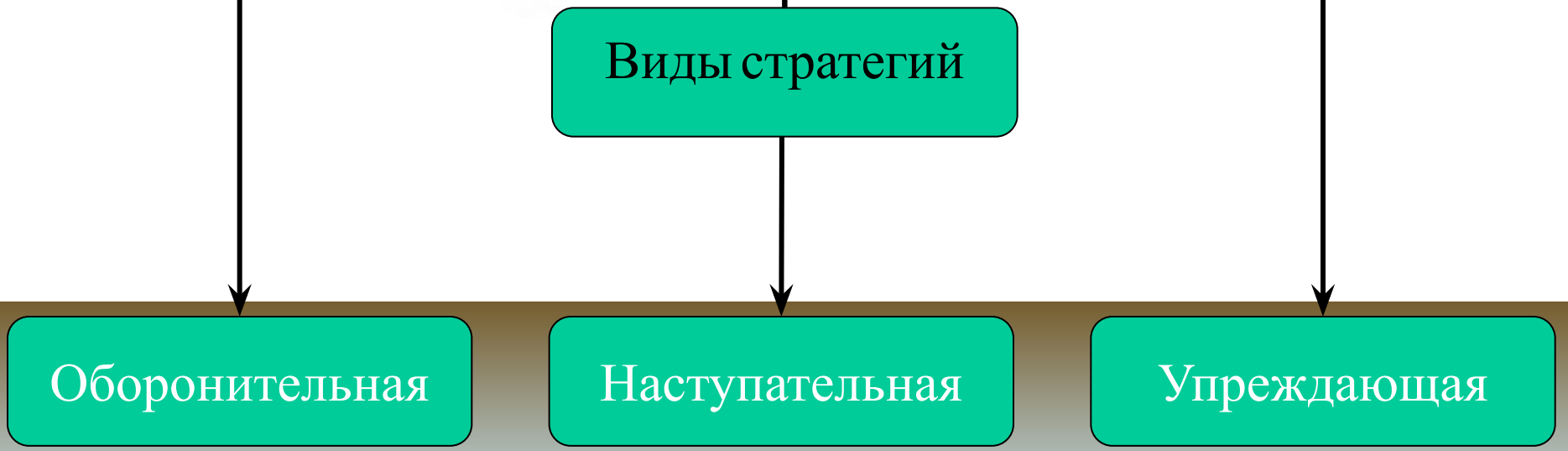
4. Блокирование каналов утечки информации;
5. Выявление закладных устройств в ТС и ПО;
6. Непрерывный контроль и управление КЗИ;
7. Обнаружение зондирований, навязываний и излучений;
8. Санкционированный доступ в физическое и информационное пространство;
9. Обнаружение возгораний, затоплений и иных ЧС;
0. Обеспечение резервирования информации;
1. Организация оборота физических носителей защищаемой информации;

Задачи Комплексной защиты информации

2. Обеспечение достоверности электронного документооборота, ЭЦП;
3. Шифрование информации на любых этапах обработки;
4. Восстановление ключевых структур при компрометации;
5. Генерация, распределение и хранение ключей и паролей;
6. Регистрация событий и обнаружение нарушений;
7. Расследование во взаимодействии с ПОО нарушений политики безопасности;
8. Непрерывный контроль и управление КЗИ.

Стратегии Комплексной защиты информации

Стратегия – общая направленность в организации деятельности с учетом объективных потребностей, возможных условий осуществления и возможностей предприятия.



Стратегии Комплексной защиты информации

Виды стратегий

Оборонительная	Наступательная	Упреждающая
защита от уже известных угроз, осуществляемая автономно, без влияния на существующую ИС	защита от всего множества потенциальных угроз	создание информационной среды, в которой угрозы не имеют условий для возникновения

Основные характеристики стратегий комплексной защиты информации

Наименование характеристики	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Возможный уровень защиты	Достаточно высок, но только в отношении известных угроз	Очень высок, но только в пределах существующих представлений о природе угроз и возможностях их проявления	Уровень защиты гарантированно очень высок
Необходимые условия реализации	Наличие методов и средств реализации	1. Наличие перечня и характеристик полного множества потенциально возможных угроз 2. Развитый арсенал методов и средств защиты 3. Возможность влиять на архитектуру ИС и технологию обработки информации	Наличие защищенных информационных технологий

Основные характеристики стратегий комплексной защиты информации

Наименование характеристики	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Ресурсоемкость	Незначительная по сравнению с другими стратегиями	Значительная (с ростом требований по защите растет по экспоненте)	1. Высокая в плане капитальных затрат 2. Незначительная в каждом конкретном случае при наличии унифицированной защищенной ИТ
Рекомендации по применению	Невысокая степень секретности защищаемой информации и не очень большие ожидаемые потери	Достаточно высокая степень секретности защищаемой информации и возможность значительных потерь при нарушении защиты	Перспективная

Этапы построения КЗИ для различных стратегий

Наименование этапов построения	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Формирование среды защиты		1. Структурированная архитектура ИС 2. Структурированная технология обработки ЗИ 3. Четкая организация работ по защите	Защищенная информационная технология в унифицированном исполнении
Анализ средств защиты	1. Представление организационной структуры ИС в виде графа, узлы – типовые структурные компоненты, а дуги – взаимосвязи между компонентами 2. Представление технологии обработки ЗИ в виде строго определенной схемы 3. Определение параметров ЗИ и условий ее обработки		

Этапы построения КЗИ для различных стратегий

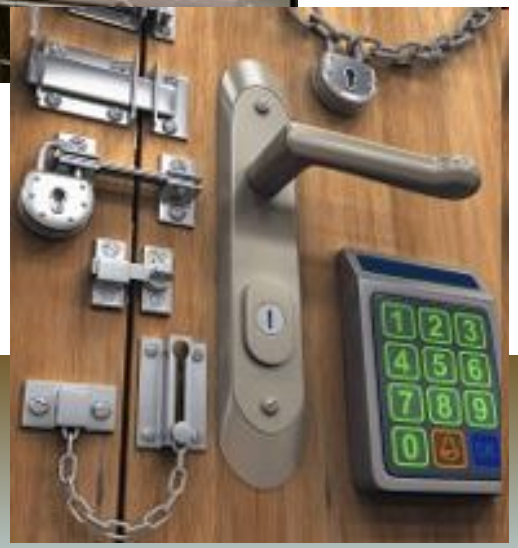
Наименование этапов построения	Стратегии комплексной защиты информации		
	Оборонительная	Наступательная	Упреждающая
Оценка уязвимости информации	1. Определение значений вероятности нарушения защиты информации в условиях ее обработки 2. Оценка размеров возможного ущерба при нарушении защиты		
Определение требований к защите	Определение вероятности нарушения защиты информации, которая должна быть обеспечена при обработке защищаемой информации		
Построение системы комплексной защиты	Определение технических средств, которые должны быть использованы при обработке ЗИ	Выбор типового варианта или проектирование индивидуальной системы КЗИ	Определение механизмов защиты, которые должны быть задействованы при создании КЗИ
Требования к среде защиты		Определяется в зависимости от требований к защите информации	Реализуется на базе унифицированной защищенной ИТ

Принципы построения КЗИ

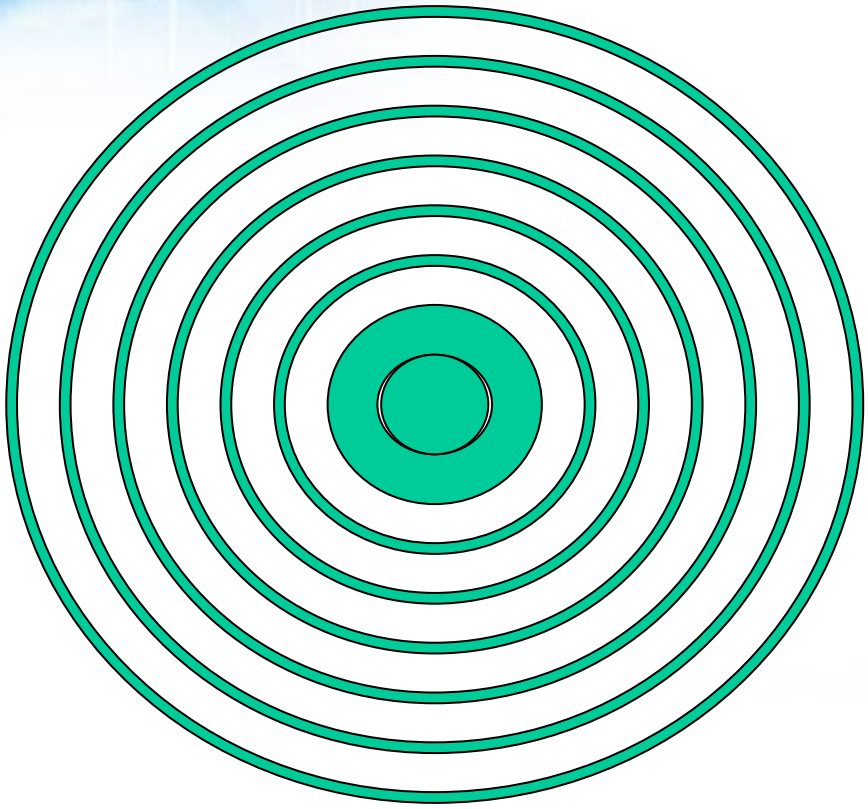
1. Простота механизма защиты
2. Постоянство защиты
3. Полнота контроля
4. Открытость проектирования
5. Идентификация
6. Разделение полномочий
7. Минимизация полномочий

Принципы построения КЗИ

8. Надежность
9. Максимальная обособленность
0. Защита памяти
1. Непрерывность
2. Гибкость
3. Неизбежность наказания нарушений
4. Экономичность
5. Специализированность



Структура Комплексной защиты информации

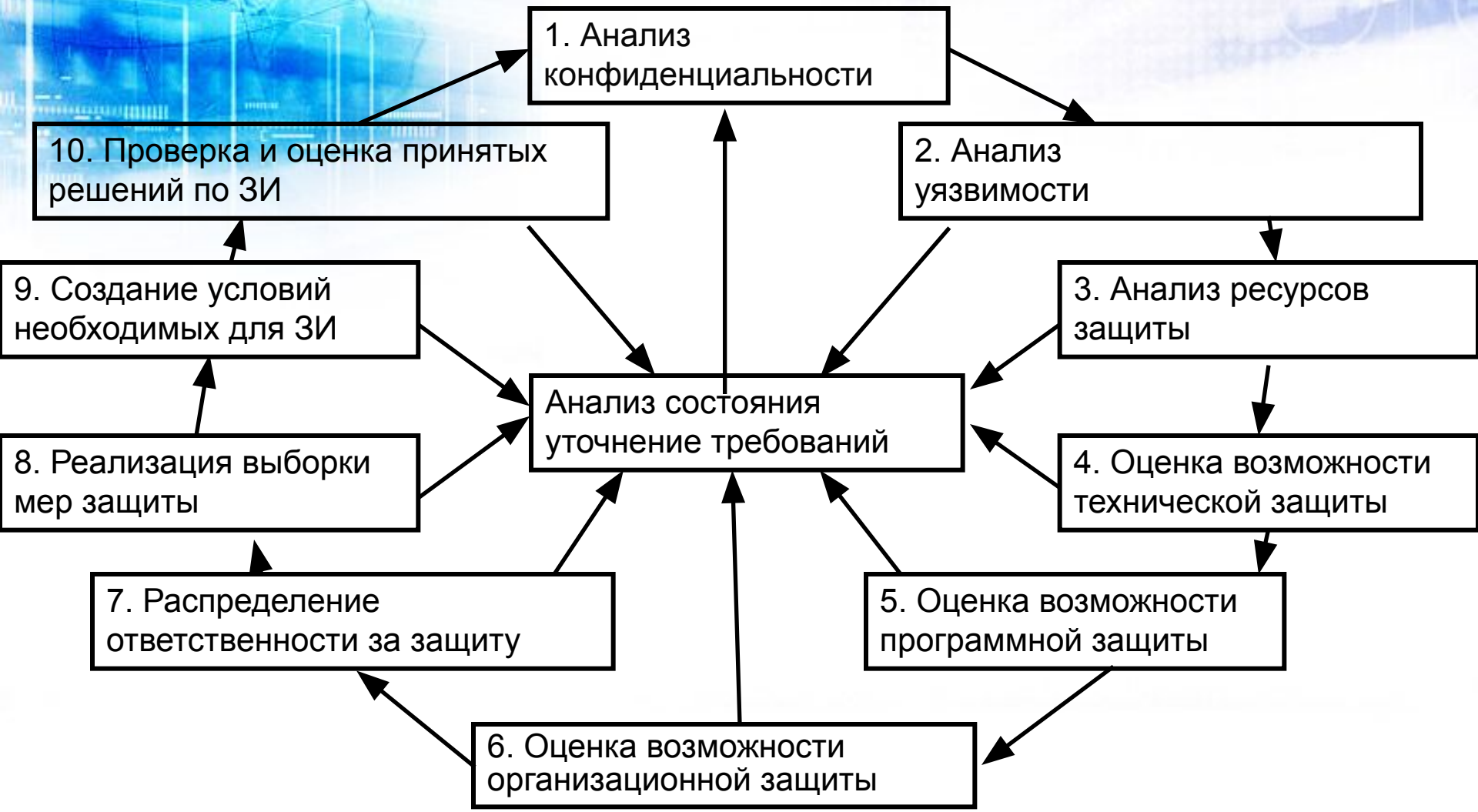


Инф
Докум
ерма
Реж
ент
Прот
им
Апп
рам
Охр
ат
Техн
ана
Инж
ика
енер
ные
соор
ужен

Основные характеристики Комплексной защиты информации

- ***Надежность***
  эшелонированность, многоуровневость
- ***Отказоустойчивость***
  минимизация последствий отказов рубежей защиты
- ***Равнопрочность***
  нарушитель должен преодолевать рубежи защиты с одинаковой трудностью, независимо от направления атаки

Основные характеристики Комплексной защиты информации



Этапы разработки Комплексной защиты информации

Разработка Политики безопасности

«Политика безопасности информации» – совокупность нормативных документов, определяющих (или устанавливающих) порядок обеспечения безопасности информации на конкретном предприятии, а также выдвигающих требования по поддержанию подобного порядка.

Цели Политики безопасности:

- формирование системы взглядов на проблему обеспечения безопасности информации и пути ее решения с учетом современных тенденций развития технологий и методов защиты информации;
- формулирование рекомендаций к повышению степени защищенности информационной системы;
- выработка общих требований к средствам защиты информации.

Уровни Политики безопасности информации

Концепция информационной безопасности
Определяет цели и задачи защиты информации

1 уровень
стратегический

Регламент обеспечения безопасности информации
Определяет организационные меры по обеспечению безопасности информации

Профиль защиты
Определяет требования к средствам защиты

2 уровень
оперативный

Инстру-кция

Руково-дство

Техниче-ские Регламенты

Задания по безопа-сности

Техниче-ское задание

3 уровень
тактиче-ский

Разработка Концепции безопасности информации

1. Определение общих положений Концепции
2. Уяснение основных направлений обеспечения безопасности информации и описание требований к безопасности информации
3. Разработка специальных глав Концепции

Разработка Регламента обеспечения безопасности информации

1. Подготовка к разработке Регламента
2. Определение общих положений Регламента
3. Определение обязанностей персонала по обеспечению безопасности информации
4. Определение правил использования компьютеров и информационных систем

Разделы Профиля защиты:

- «Введение ПЗ»;
- «Описание Объекта Оценки»;
- «Среда безопасности ОО».
- «Цели безопасности»;
- «Требования безопасности ИТ»;
- «Обоснование».

Разработка Профиля защиты

Профиль защиты включает:

- ✔ формулировку необходимости ИБ;
- ✔ описание среды, в которой находится КИС;
- ✔ описание предположений о существующем состоянии безопасности;
- ✔ описание политики безопасности, которая должна выполняться;
- ✔ описание целей безопасности;
- ✔ функциональные требования к безопасности и требования доверия к безопасности;
- ✔ обоснование достаточности функциональных требований и требований доверия к безопасности.

Безопасность ценных информационных ресурсов

Цель ИБ – безопасность информационных ресурсов в любой момент времени в любой обстановке.

Первоначально всегда необходимо решить следующие вопросы:

Что защищать?
Почему защищать?
От кого защищать?
Как защищать?

Безопасность ценных информационных ресурсов

Ранее главные опасности:

- утрата конфиденциального документа;
- разглашение конфиденциальных сведений;
- утечка по техническим каналам.

В настоящее время главные опасности:

- незаконное тайное оперирование электронными документами без кражи из БД;
- незаконное использование информационных ресурсов для извлечения материальной выгоды.

Безопасность ценных информационных ресурсов

Архитектура систем защиты информации

- Электронные информационные системы;
- Весь комплекс управления предприятием в единстве его функциональных и структурных систем;
- Традиционные документационные процессы

Обязательные элементы СЗИ:

- правовые;
- организационные;
- инженерно-технические;
- программно-аппаратные;
- криптографические.

Критерии ценности информации

Виды ценной информации:

1. ***Техническая и технологическая:***

- химическая формула;
- рецепт;
- результат испытаний;
- данные контроля качества;
- методы изготовления продукции;
- производственные показатели.

Критерии ценности информации

2. Деловая:

- управленческие решения;
- методы реализации функций;
- стоимостные показатели;
- результаты исследования рынка;
- списки клиентов;
- экономические прогнозы.

Основные направления формирования ценной информации

1. Управление предприятием
2. Прогнозирование и планирование
3. Финансовая деятельность
4. Производственная деятельность
5. Торговая деятельность
6. Переговоры и совещания по направлениям деятельности

Основные направления формирования ценной информации

7. Формирование ценовой политики
8. Формирование состава клиентов, компаньонов и т.д.
9. Изучение направлений интересов конкурентов
0. Участие в торгах и аукционах
1. Научная и исследовательская деятельность
2. Использование новых технологий
3. Управление персоналом
4. Организация безопасности предприятия

Выявление конфиденциальных сведений

Основополагающая часть системы комплексной защиты информации – процесс выявления и регламентации состава конфиденциальной информации.

Критерии анализа информационных ресурсов:

- степень заинтересованности конкурентов;
- степень ценности (стоимостной, правовой аспект).

Предпосылки отнесения информации к конфиденциальным сведениям

1. Не отражает негативные стороны деятельности фирмы (нарушение законодательства и фальсификацию финансовой деятельности с целью неуплаты налогов);
2. Не общедоступна и не общеизвестна;
3. Возникновение или получение информации законно и связано с расходованием материального, финансового и интеллектуального потенциала;
4. Персонал знает о ценности информации и обучен правилам работы с ней;
5. Предприниматель выполняет реальные действия по защите конфиденциальной информации.

Перечень конфиденциальных сведений

Перечень – классифицированный список типовой и конкретно ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах.

Перечень конфиденциальных сведений

- ✔ закрепляет факт отнесения сведений к защищаемой информации;
- ✔ определяет срок, период недоступности этих сведений,
- ✔ уровень конфиденциальности (гриф);
- ✔ список должностей, которым дано право использовать эти сведения в работе.

Документирование конфиденциальных сведений

Основные отличия документированных конфиденциальных сведений:

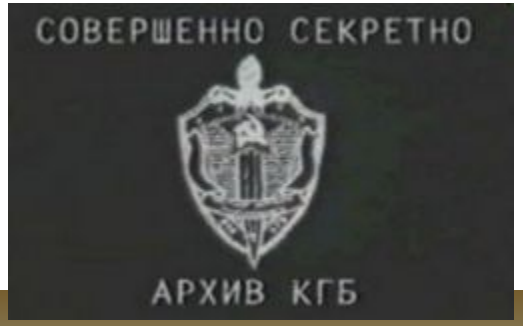
1. Обязательность получения разрешения на документирование конфиденциальной информации от полномочного руководителя;
2. Установления грифа (уровня) конфиденциальности сведений, подлежащих включению в документ;

Документирование конфиденциальных сведений

3. Оформление и учет носителя для документирования, выделенного комплекса конфиденциальных сведений;
4. Учет подготовленного черновика документа;
5. Составление черновика и вариантов текста документа;
6. Получение разрешения на изготовление документа от полномочного руководителя;
7. Изготовление проекта конфиденциального документа;
8. Издание конфиденциального документа.

Угрозы конфиденциальным документам

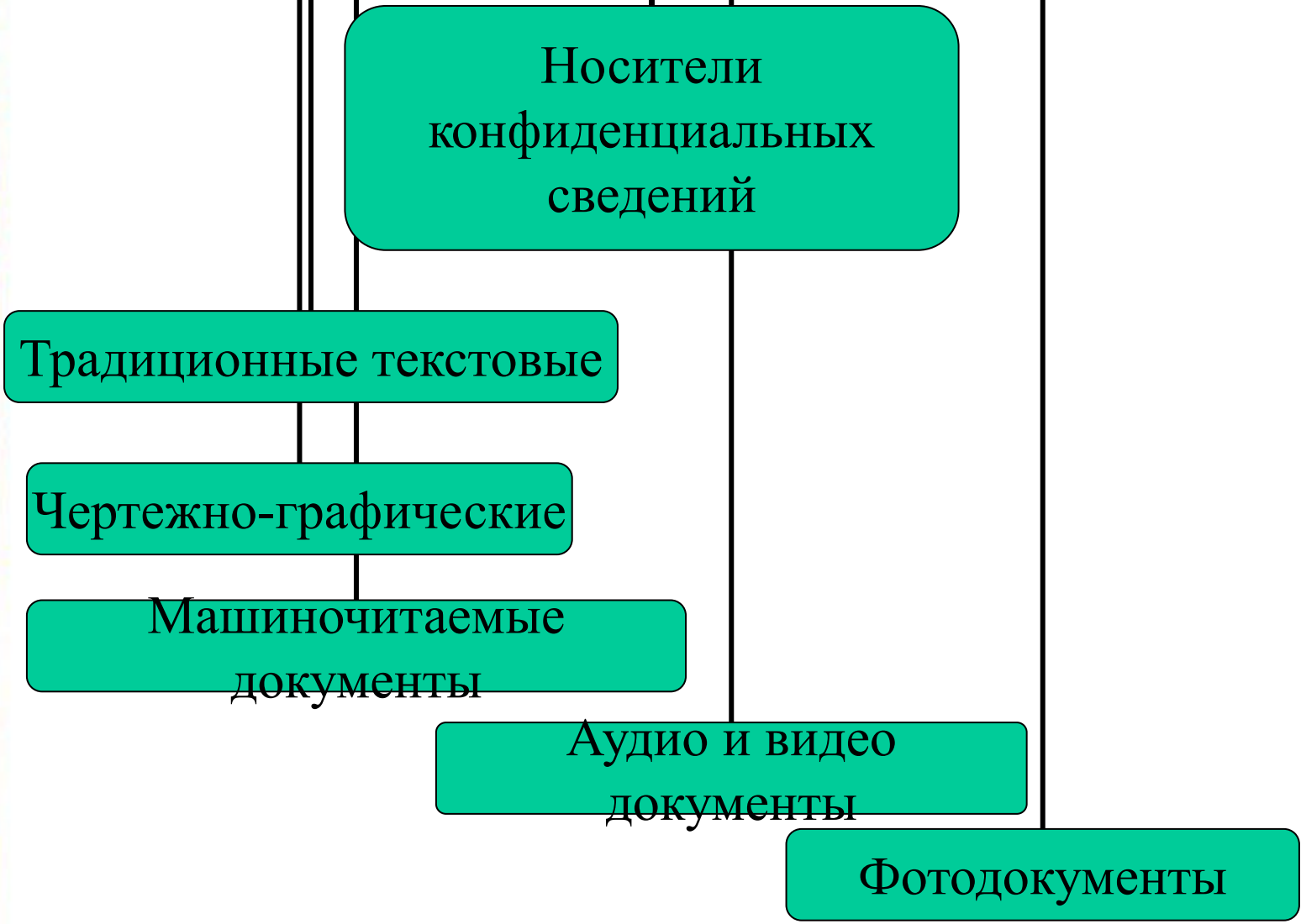
1. Документирование на случайном носителе;
2. Подготовка к изданию документа, не обоснованная деловой необходимостью или не разрешенного документирования;
3. Включение в документ избыточной информации;
4. Случайное (умышленное) занижение грифа конфиденциальности;



Угрозы конфиденциальным документам

5. Изготовление документа в условиях, не гарантирующих конфиденциальности обрабатываемой информации;
6. Утеря оригинала, черновика, варианта или редакции документа;
7. Попытка подмены утраченного материала;
8. Сообщение содержимого проекта документа постороннему лицу;
9. Несанкционированное копирование;
10. Утечка информации по техническим каналам;
11. Ошибочные действия пользователей.

Носители конфиденциальных сведений



Задачи учета конфиденциальных документов

1. Закрепление факта присвоения носителю категории ограничения доступа;
2. Присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки наличия;

Задачи учета конфиденциальных документов

3. Документирование фактов перемещения носителей между руководителями и сотрудниками;
4. Закрепление персональной ответственности за сохранность носителя;
5. Контроль работы исполнителей над документами и своевременное уничтожение при потере практической ценности.

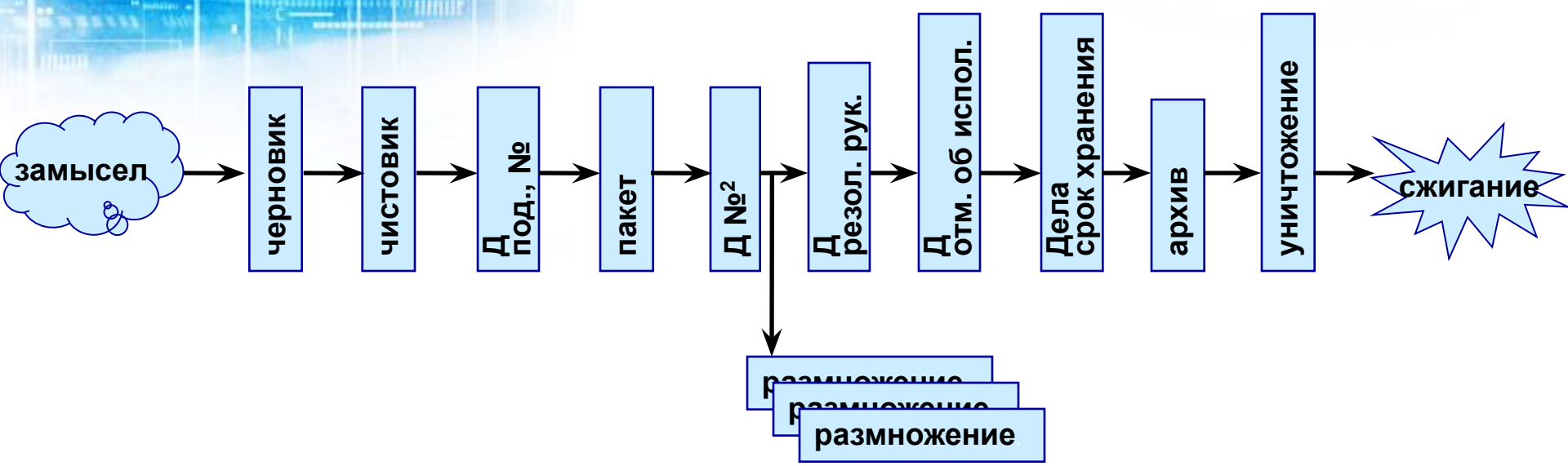
Конфиденциальные документы: состав и период нахождения документов в делах

Конфиденциальный документ – необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического (физического) лица.

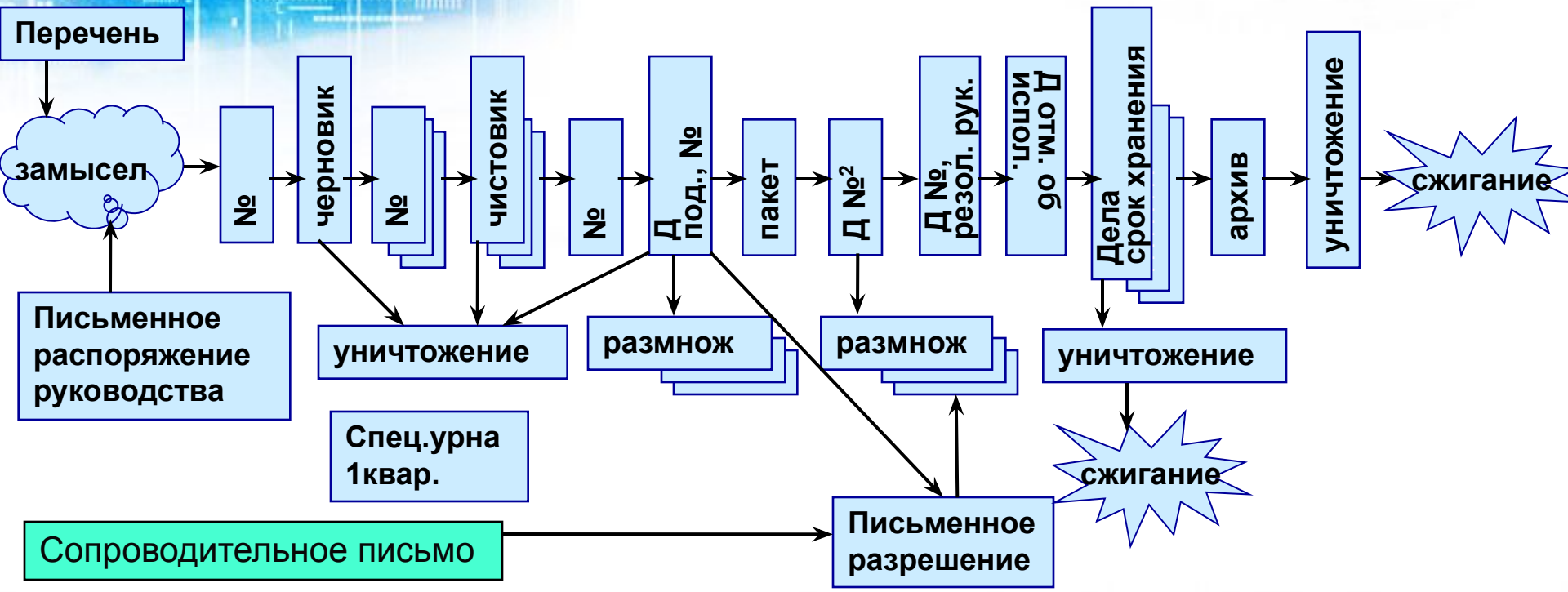
Периоды нахождения конфиденциальных документов в делах:

- При сроке от 1 до 3 лет − кратковременный
- При сроке более 3 лет − долговременный

Жизненный цикл конфиденциального документа



Жизненный цикл конфиденциального документа



Проверка наличия: ежедневный учет; квартальное движение; годовое наличие

Проверка вне плана: отпуск, болезнь, командирован, смена исполнителя (ответственного лица), утрата или повреждение оттисков печати.

Доступ к конфиденциальному документу

Работники предприятия, допущенные к конфиденциальным сведениям и документам, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с памяткой о сохранении коммерческой тайны предприятия.

Памятка составляется службой безопасности с учётом специфики конкретного предприятия, подписывается заместителем директора и утверждается директором предприятия.

Оформление конфиденциального документа

Все документы, содержащие коммерческую тайну или конфиденциальную информацию, подлежат учёту и специальному обозначению.

На документе проставляют *гриф ограничения доступа с указанием номера экземпляра*, *обладателя этой информации* (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.

Пример оформления конфиденциального документа

Коммерческая тайна
Экз. № 1
ЗАО «Парус»
Ул. Марса, 78
Москва, 123456

Такие грифы показывают, что право собственности на информацию, содержащуюся в документе, принадлежит предприятию и охраняется законодательно.

Оформление конфиденциального документа

На документе с грифом «Коммерческая тайна» указывается количество экземпляров документа и место нахождения каждого из них (ниже реквизитов «подпись» и «отметка об исполнителе»)

На обороте листа документа, имеющего гриф, руководитель пишет фамилии тех должностных лиц, которым разрешено пользоваться этим документом

Пример оформления конфиденциального документа

Разрешаю:
В.В. Иванову
П.С. Путину

Подпись руководителя

Дата

Ограничения по конфиденциальным документам

При работе с конфиденциальными документами необходимо ввести ряд следующих ограничений для работников предприятия:

- запрещается делать выписки из документов, имеющих гриф ограничения доступа, без письменного разрешения руководителя;

- запрещается знакомиться с документами, делами, информацией, содержащейся в памяти компьютера, других работников предприятия;

Ограничения по конфиденциальным документам

- запрещается использовать информацию из документов, имеющих гриф ограниченного доступа, в открытых докладах, сообщениях, переписке, рекламных изданиях;

- запрещается предоставлять свой компьютер для работы другим сотрудникам предприятия и работать на их ПК;

- запрещается бесконтрольно оставлять конфиденциальные документы на рабочем столе и работающий компьютер с конфиденциальной информацией.

Конфиденциальный документ

Документ, содержащий сведения конфиденциального характера, попавший в руки конкурентов, может нанести огромный ущерб предприятию.

Определённые виды информации, например, финансовая, ноу-хау, данные о персонале или договорах нуждаются в особой защите.

Причиной утечки информации могут стать копии и черновики документов, выброшенные в корзину для бумаг, небрежно разбросанные на рабочих столах, и даже неправильно утилизированные документы, предназначенные для уничтожения.

Поэтому так важно уничтожать документацию без возможности её восстановления.

Конфиденциальный документ

Для этой цели используют специальные устройства – ***уничтожители*** или ***шредеры*** (от англ. яз. – резать, рвать, уничтожать).

По способам резки уничтожители документов подразделяются на два типа:

* с параллельной резкой – резка на полосы различной ширины;

* с перекрёстной (продольно – поперечной) резкой на более мелкие фрагменты.

Уничтожение конфиденциального документа

Шредер выбирается в зависимости от уровня секретности используемых на предприятии документов.

Чем выше степень измельчения уничтоженного документа, тем сложнее его восстановить.

Обеспечение сохранности конфиденциального документа

Для обеспечения сохранности и неразглашения конфиденциальных сведений предприятия необходимо:

- выполнение самых простых требований безопасности

- профессиональное обучение персонала требованиям работы с конфиденциальными документами

- материальное стимулирование руководством организации сотрудников, имеющих доступ к документам с грифом «Конфиденциально»

Обеспечение сохранности конфиденциального документа

- правильная организация секретного делопроизводства и документооборота на предприятии

- строгое привлечение к ответственности сотрудников предприятия за нарушение норм и инструкций по секретному делопроизводству.

- сведения к минимуму несанкционированного доступа к конфиденциальной документации можно достичь путём увеличения различных административных, технологических и других барьеров.