Вопрос 6. Программные и технические средства защиты информации.

Комплексно-системный подход к защите информации.

В России классификация систем защиты определяется руководящим документом Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». В соответствии с этим документом устанавливается семь классов защищенности средств вычислительной техники от несанкционированного доступа к информации. Самый низкий класс - седьмой, самый высокий - первый.

Защита информации предполагает комплексный и системный подход. Только взаимообусловленный, основанный на тщательном анализе самой компьютерной системы, комплекс защитных мер может обеспечить достаточный уровень безопасности обрабатываемой в автоматизированной информационной системе (АИС) информации. Любое происшествие или успешная атака являются, как правило, следствием совокупности причин, реализацией нескольких угроз.

Перечисленные требования в системе защиты автоматизированной информационной системы способны противостоять большинству угроз компьютерной информации, связанных с несанкционированным доступом злоумышленника на программном и аппаратном уровнях. Требования к системе защиты информации и меры по их реализации сформулированы в табл. 7.8.1.

Таблица 7.8.1. Требования к системе защиты информации и меры по их реализации

Требования к системе защиты компьютерной системы	Методы защиты информации							
	идентификация и аутентификация	ограничение доступа на вход в систему	разграничение доступа	регистрация событий (аудит)	криптографическая защита	контроль целостности	управление политикой безопасности	уничтожение «технологического мусора»
1. Только зарегистрированные пользователи в разрешенное время могут загрузить ОС	+	+					+	
2. Без регистрации никто не должен получать доступ к конфиденциальной информации	+	+	+		+		+	+
3. Пользователь должен быть уверен в «чистоте» компьютерной системы		+	+			+	+	
4. Пользователи должны получать доступ только к той информации и с теми возможностями, которые соответствуют их функциональным обязанностям			+				+	
5. Пользователям разрешается применение только необходимых для обработки информации программных средств			+				+	
6. Для хранения конфиденциальных данных должны использоваться только учтенные носители			+				+	

7. Конфиденциальная информация, в том числе ее фрагменты в виде «технологического мусора», не должна быть доступна иному субъекту	+	+	+		+		+	+
8. В АИС автоматически должна вестись регистрация наиболее важных событий	+	+		+			+	
9. При печати документов на бумажные носители автоматически должны фиксироваться факт распечатки в специальном журнале и выводиться штамп на сам документ				+			+	
10. В АИС должен быть администратор безопасности, который обязан воплощать в жизнь политику безопасности							+	

В таблице 7.8.1 не учитываются методы защиты, которые не связаны непосредственно с выполнением указанных требований: антивирусная защита, резервирование данных, сетевая защита, защита от утечки и перехвата информации по техническим каналам. В данной таблице символом S обозначено, какие требования позволяет обеспечить тот или иной метод защиты. Из таблицы видно, что нет требований, которые не обеспечиваются ни одним из рассмотренных выше методов защиты. Хотя бы один из методов защиты реализует каждое из требований.

Наиболее важные требования обеспечиваются выполнением одновременно нескольких методов. В этом проявляется комплексный подход к защите компьютерной информации. Необходимость комплексного и системного подхода наглядно иллюстрируется на примере требования 2 - без регистрации никто не должен получать доступ к конфиденциальной информации. Методы, обеспечивающие выполнение этого требования, взаимосвязаны. Без достоверной аутентификации субъекта АИС не допустима загрузка операционной системы. Без идентификации и аутентификации пользователя также не имеют смысла регистрация сеанса его работы и реализация той или иной модели разграничения доступа.

В то же время, если злоумышленник получит физический доступ, например, к жесткому диску, то с помощью низкоуровневых дисковых редакторов он сумеет считать приватные данные в обход системы разграничения доступа. Противодействием атакам наиболее подготовленных злоумышленников может стать криптографическая защита информации. С другой стороны, правомерность обращения субъекта к самим программам шифрования, процесс ввода ключевой (аутентифицирующей) информации, блокирование вредоносных программ - перехватчиков паролей, находятся под контролем систем ограничения и разграничения доступа. Таким образом, криптографическое преобразование конфиденциальных данных только в тесной взаимосвязи с механизмами ограничения и разграничения доступа способны гарантировать надежную защиту компьютерной информации от НСД. Этот же комплект методов защиты противодействует «программной» утечке конфиденциальной информации, обусловленной несовершенством операционных систем, в том числе наличием «технологического мусора» (требование 7).

Не менее показательным является требование аудита критических событий в АИС. На первый взгляд это требование может показаться обособленным и независимым от других требований и методов, их реализующих. Однако каким образом регистрировать, например, попытки несанкционированного входа в систему, если вход в нее не ограничен? Безусловно, само знание факта злоумышленных (подозрительных) действий в АИС важно для их пресечения. Фиксация конкретного лица, совершившего эти действия, позволит расследовать правонарушения и вести их профилактику более эффективно. Как выявлять

злоумышленников, если в системе не ведутся идентификация и аутентификация пользователей?

Система защиты информации АИС - совокупность разнообразных средств и методов, взаимообусловливающих и дополняющих друг друга. Разумная, взвешенная, комплексная их реализация - непростая и творческая задача. Программно-аппаратные средства защиты информации помогают решить ее более целенаправленно и эффективно.

Осуществляя построение и эксплуатацию защищенной компьютерной системы, необходимо базироваться на принятой в организации политике безопасности, на представлении методов защиты компьютерной информации, с помощью которых могут быть реализованы требования политики безопасности, и на этой основе выбирать, устанавливать и администрировать специализированные программно-аппаратные средства защиты информации.

Средства защиты информации (СЗИ) - технические, криптографические, программные и другие средства, предназначенные для реализации совокупности взаимосвязанных требований безопасности АС, а также средства контроля эффективности защиты информации. СЗИ являются надстройкой над программно-аппаратной средой защищаемой компьютерной системы и самостоятельно или совместно со встроенными возможностями операционных систем и аппаратных устройств АС реализуют некоторый набор защитных механизмов.

Программные средства защиты информации.

Программно-аппаратные средства защиты информации призваны реализовывать несколько мер и соответствующих им методов по противодействию злоумышленнику при возможности его физического доступа к компьютерам автоматизированной системы.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения компьютерных систем исключительно для выполнения защитных функций.

Программные средства защиты информации создаются в результате разработки специального программного обеспечения, которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы.

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей компьютерных систем;
- программы разграничения доступа пользователей к ресурсам компьютерных систем;
- программы шифрования информации;
- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т.п.) от несанкционированного изменения, использования и копирования.

Программные средства включают в себя:

- парольный доступ-задание полномочий пользователя;
- блокировка экрана и клавиатуры, например с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;
- использование средств парольной защиты BIOS на сам BIOS и на ПК в целом и т.д.

Надо понимать, что под идентификацией, применительно к обеспечению информационной безопасности компьютерных систем, понимают однозначное распознавание уникального имени субъекта компьютерных систем. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Также к программным средствам защиты информации относятся:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью компьютерных систем, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

- программы тестового контроля защищенности компьютерных систем и др.

Под криптографическим способом защиты информации подразумевается ее шифрование при вводе в компьютерную систему.

На практике обычно используются комбинированные способы защиты информации от несанкционированного доступа.

Среди механизмов безопасности сетей обычно выделяют следующие основные:

- шифрование;
- контроль доступа;
- цифровая подпись.

Шифрование применяется для реализации служб засекречивания и используется в ряде других служб.

Механизмы контроля доступа обеспечивают реализацию одноименной службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется в точке инициализации связи, в промежуточных точках, а также в конечной точке.

Механизмы контроля доступа делятся на две основные группы:

- аутентификация объектов, требующих ресурса, с последующей проверкой допустимости доступа, для которой используется специальная информационная база контроля доступа;

- использование меток безопасности, наличие у объекта соответствующего мандата дает право на доступ к ресурсу.

Самым распространенным и одновременно самым ненадежным методом аутентификации является парольный доступ. Более совершенными являются пластиковые карточки и электронные жетоны. Наиболее надежными считаются методы аутентификации по особым параметрам личности, так называемые биометрические методы.

Цифровая подпись по своей сути призвана служить электронным аналогом ручной подписи, используемой на бумажных документах. Правила использования электронной цифровой подписи регулируются Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

Дополнительными механизмами безопасности являются следующие:

- обеспечение целостности данных;
- аутентификация;
- подстановка графика;
- управление маршрутизацией;
- арбитраж.

Механизмы обеспечения целостности данных применимы как к отдельному блоку данных, так и к потоку данных. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Возможны и более простые методы контроля целостности потока данных, например нумерация блоков, дополнение их меткой имени и т.д.

В механизме обеспечения аутентификации различают постороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов одного уровня проверяет подлинность другого, тогда как во втором - проверка является взаимной. На практике часто механизмы аутентификации, как правило, совмещаются с контролем доступа,

шифрованием, цифровой подписью и арбитражем.

Механизмы подстановки трафика основываются на генерации объектами сети фиктивных блоков, их шифровании и организации их передачи по каналам сети.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по сети.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами сети, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтвердить упомянутые характеристики.

В общем случае для реализации одной службы безопасности может использоваться комбинация нескольких механизмов безопасности.

Большинство систем защиты имеют в своем распоряжении средства управления системным журналом (audit trail). Как было показано выше, системный журнал является составной частью монитора ссылок и служит для контроля соблюдения политики безопасности. Он является одним из основных средств контроля, помогающим администратору предотвращать возможные нарушения в связи с тем, что:

- способен оперативно фиксировать происходящие в системе события;
- может помочь выявить средства и априорную информацию, использованные злоумышленником для нарушения;
- может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Содержимое системного журнала и других наборов данных, хранящих информацию о результатах контроля, должны подвергаться периодическому просмотру и анализу (аудит) с целью проверки соблюдения политики безопасности.

Средства регистрации событий также являются обязательной компонентой системы разграничения доступа. Журналы регистрации событий располагаются на ВЗУ. В таких журналах записываются данные о входе пользователей в систему и о выходе из нее, обо всех попытках выполнения несанкционированных действий, о доступе к определенным ресурсам и т. п. Настройка журнала на фиксацию определенных событий и периодический анализ его содержимого осуществляется дежурным оператором и вышестоящими должностными лицами. Процесс настройки и анализа журнала целесообразно автоматизировать программным путем.

Непосредственное управление системами разграничения доступа осуществляет дежурный оператор комплексной системы защиты информации, который, как правило, выполняет и функции дежурного администратора компьютерной системы. Он загружает ОС, обеспечивает требуемую конфигурацию и режимы работы компьютерной системы, вводит в систему разграничения доступа полномочия и атрибуты пользователей, осуществляет контроль и управляет доступом пользователей к ресурсам компьютерной системы.

Журнал может просматриваться только администратором. Для проверки работоспособности системы используются программы тестирования. При необходимости пользователь может закрыть информацию на своем диске и от администратора, зашифровав последнюю средствами абонентского шифрования.

Имеется возможность просмотра журналов IIS и журналов безопасности Windows для контроля за событиями безопасности в течение длительных промежутков времени. Для просмотра журналов безопасности Windows можно использовать Microsoft Management Console. Журналы IIS могут быть просмотрены с помощью любого текстового редактора или текстового процессора. Для получения дополнительных сведений о просмотре журналов IIS см. раздел Ведение журналов узлов.

В журнале безопасности Windows попытки несанкционированного доступа фиксируются как записи о предупреждениях или ошибках. Эти журналы могут быть

заархивированы для дальнейшего использования.

Чтобы выявить возможные проблемы безопасности с помощью просмотра журнала безопасности Windows

Нажмите кнопку Пуск, выберите команды Настройка и Панель управления, дважды щелкните компонент Администрирование, а затем дважды щелкните значок Управление компьютером.

Раскройте узел Служебные программы.

Раскройте узел Просмотр событий.

Выберите Безопасность.

Примечание. Невозможность просмотреть журнал безопасности свидетельствует о том, что используемая учетная запись пользователя не имеет привилегий для выполнения этой операции. Это может происходить из-за того, что политика безопасности уровня домена перекрывает политику безопасности уровня компьютера. Это означает, что можно войти в систему как администратор локального компьютера, но не иметь доступа к журналу безопасности. Чтобы получить эти разрешения, обратитесь к администратору сети. Для получения информации о политике безопасности см. документацию Windows.

Проверьте журналы на наличие подозрительных событий безопасности, в том числе следующих:

Недопустимые попытки входа в систему.

Неудачное использование привилегий.

Неудачные попытки доступа к файлам .bat или .cmd и их изменения.

Попытки изменения привилегий безопасности или журнала аудита.

Попытки завершения работы сервера.

Чтобы заархивировать журнал безопасности Windows

Нажмите кнопку Пуск, выберите команды Настройка и Панель управления, дважды щелкните компонент Администрирование, а затем дважды щелкните значок Управление компьютером.

Раскройте узел Служебные программы.

Раскройте узел Просмотр событий.

Выберите Безопасность.

В меню Действие выберите команду Сохранить файл журнала как.

В диалоговом окне Сохранить как выберите каталог, в котором будет сохраняться файл, и введите имя файла.

Примечание. Журнал безопасности может быть сохранен как файл событий (.evt), текстовый файл (.txt), или файл с разделителями-запятыми (.csv).

Чтобы открыть заархивированный журнал безопасности Windows.

Нажмите кнопку Пуск, выберите команды Настройка и Панель управления, дважды щелкните компонент Администрирование, а затем дважды щелкните значок Управление компьютером.

Раскройте узел Служебные программы.

Раскройте узел Просмотр событий.

Выберите Безопасность.

В меню Действие выберите команду Создать вид журнала.

В диалоговом окне Добавление нового представления журнала выберите переключатель Сохраненный (представление ранее созданного журнала) и выберите файл.

В раскрывающемся списке Тип журнала выберите Безопасность.

Чтобы открыть файл в обозревателе, нажмите кнопку ОК.

Чтобы выявить возможные проблемы безопасности с помощью просмотра файлов журналов IIS

В текстовом редакторе, например в «Блокноте», откройте файл журнала. Для

получения дополнительных сведений о файлах журналов см. раздел Ведение журналов узлов.

Проверьте журналы на наличие подозрительных событий безопасности, в том числе следующих:

Многочисленные невыполненные команды с попытками запуска исполняемых файлов или сценариев. (Следует более тщательно проследить за каталогом со сценариями.)

Многочисленные неудачные попытки входа с одного IP-адреса, возможной целью которых является увеличение интенсивности сетевой передачи данных или помехи для доступа других пользователей.

Неудачные попытки доступа к файлам .bat или .cmd и их изменения.

Несанкционированные попытки передачи файлов в каталог, содержащий исполняемые файлы.

К преимуществам программных средств защиты информации относятся:

- простота тиражирования;
- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных компьютерных систем);
- простота применения - одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя ни каких новых (по сравнению с другими программами) навыков;
- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

К недостаткам программных средств защиты информации относятся:

- снижение эффективности компьютерных систем за счет потребления ее ресурсов, требуемых для функционирования программ защиты;
- более низкая производительность (по сравнению с выполняющими аналогичные функции техническими средствами защиты, например шифрования);
- пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение компьютерных систем), что создает для нарушителя принципиальную возможность их обхода;
- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации компьютерных систем.

Технические средства защиты информации.

В Постановлении Правительства РФ от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" под технической защитой конфиденциальной информации понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

К техническим средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств компьютерных систем и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к техническим, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств компьютерных систем.

К основным техническим средствам защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);
- устройства для шифрования информации;

- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных технических средств защиты информации:

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей компьютерных систем и др.

Технические средства привлекают все большее внимание специалистов не только потому, что их легче защитить от повреждений и других случайных или злоумышленных воздействий, но еще и потому, что техническая реализация функций выше по быстродействию, чем программная, а стоимость их неуклонно снижается.

На рынке технических средств защиты появляются все новые устройства. Ниже приводится в качестве примера описание электронного замка.

- идентификация и аутентификация пользователей;
- контроль целостности файлов и физических секторов жесткого диска;
- блокировка входа в систему зарегистрированного пользователя при превышении им заданного количества неудачных попыток входа;
- регистрация событий, имеющих отношение к безопасности системы.

Контроль целостности предназначен для того, чтобы убедиться, что программы и файлы пользователя и особенно системные файлы ОС не были модифицированы злоумышленником или введенной им программной закладкой. Для этого в первую очередь в работу вступает разборщик файловой системы ОС. Построение же списка контроля целостности объектов выполняется с помощью утилиты ОС, что в принципе дает возможность программе-перехватчику модифицировать этот список, а ведь хорошо известно, что общий уровень безопасности системы определяется уровнем защищенности самого слабого звена.

Организационную структуру системы технической защиты информации ограниченного доступа в организации образуют:

- отдел защиты информации - в части методического руководства и организации мероприятий по технической защите информации ограниченного доступа;
- структурные подразделения (штатные специалисты) по защите информации организации - в части реализаций мер технической защиты информации ограниченного доступа в организации.

Мероприятия по технической защите информации ограниченного доступа являются составной частью деятельности организации и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности и конфиденциальности проводимых работ с информацией ограниченного доступа.

Ответственность за организацию и своевременную реализацию эффективных мер по технической защите информации ограниченного доступа возлагается на руководителей организации и руководителей подотчетных им подразделений.

Техническая защита информации ограниченного доступа осуществляется путем выполнения комплекса мероприятий, направленных на предотвращение:

- утечки информации ограниченного доступа по техническим каналам за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами;
- несанкционированного доступа к обрабатываемой, хранящейся в технических средствах и передаваемой по каналам связи информации ограниченного доступа;
- преднамеренных программно-технических воздействий с целью хищения, разрушения (уничтожения), искажения информации ограниченного доступа в процессе обработки, передачи и хранения;
- перехвата техническими средствами речевой информации ограниченного доступа из

помещений.

Объектами, подлежащими технической защите, являются:

- информационные ресурсы, представленные в виде носителей на магнитной и оптической основах, информативных физических полей, информационных массивов и баз данных и содержащие информацию ограниченного доступа;
- технические средства обработки и передачи информации ограниченного доступа;
- помещения, предназначенные для обработки информации ограниченного доступа и проведения секретных (конфиденциальных) переговоров.

Основными организационно-техническими мероприятиями по технической защите информации ограниченного доступа являются:

- категорирование объектов в зависимости от их важности, степени секретности (конфиденциальности) информации ограниченного доступа и условий эксплуатации, а также классификация автоматизированных систем по требованиям защищенности от несанкционированного доступа к информации ограниченного доступа;
- разработка и внедрение решений по технической защите информации ограниченного доступа при создании и эксплуатации объектов;
- применение информационных и автоматизированных систем управления в защищенном исполнении;
- организация аттестации объектов, по требованиям безопасности информации ограниченного доступа;
- обеспечение физической защиты объектов;
- обеспечение защиты информации ограниченного доступа от утечки по техническим каналам при ее обработке, хранении и передаче;
- обеспечение защиты информации ограниченного доступа от несанкционированного доступа к ней в автоматизированных информационных системах и локальных вычислительных сетях, а также от компьютерных вирусов;
- совершенствование методической базы обеспечения информационной безопасности;
- организация и проведение контроля состояния технической защиты информации ограниченного доступа.

Совокупность технологических стадий (функциональных элементов), сопровождающих потоки конфиденциальных документов, несколько отличается от аналогичной совокупности, свойственной потокам открытых документов. Так, входной документопоток включает в себя следующие стадии обработки конфиденциальных сведений:

Прием, учет и первичная обработка поступивших пакетов, конвертов, незаконвертованных документов;

Учет поступивших документов и формирование справочно-информационного банка данных по документам;

Предварительное рассмотрение и распределение поступивших документов;

Рассмотрение документов руководителям! и передача документов на исполнение;

Ознакомление с документами исполните лей, использование или исполнение документов.

Выходной и внутренний документопотоки включают в себя следующие стадии обработки конфиденциальных документов:

Исполнение документов (этапы: определение уровня грифа конфиденциальности предполагаемого документа, учет носителя будущего документа, составление текста, учет подготовленного документа, его изготовление и издание);

Контроль исполнения документов;

Обработка изданных документов (экспедиционная обработка документов и отправка их адресатам; передача изданных внутренних документов на исполнение);

Систематизация исполненных документов в соответствии с номенклатурой дел,

оформление, формирование и закрытие дел;

Подготовка и передача дел в ведомственный архив (архив фирмы).

В состав всех документопотоков включается также ряд дополнительных стадий обработки конфиденциальных документов:

Инвентарный учет документов, дел и носителей информации, не включаемых в номенклатуру дел;

Проверка наличия документов, дел и носителей информации;

Копирование и тиражирование документов;

Уничтожение документов, дел и носителей информации.

Стадии, составляющие тот или иной документопоток, реализуются специализированной технологической системой обработки и хранения конфиденциальных документов.

Под технологической системой обработки и хранения конфиденциальных документов понимается упорядоченный комплекс организационных и технологических процедур и операций, предназначенных для практической реализации задач, стоящих перед функциональными элементами (стадиями) документопотока. Технология обработки и хранения конфиденциальных и открытых документов базируется на единой научной и методической основе, призванной решать задачи обеспечения документированной информацией управленческие и производственные процессы. Одновременно технологическая система обработки и хранения конфиденциальных документов решает и другую не менее важную задачу - обеспечение защиты носителей информации и самой информации от потенциальных и реальных угроз их безопасности.

В отличие от открытых документов к обработке конфиденциальных документов предъявляются следующие серьезные требования, которые в определенной степени гарантируют решение указанных задач:

Централизации всех стадий, этапов, процедур и операций по обработке и хранению конфиденциальных документов;

Учета всей без исключения конфиденциальной информации;

Операционного учета технологических действий, производимых с традиционным (бумажным) или электронным носителем (в том числе чистым) и документом, учет каждого факта «жизненного цикла» документа;

Обязательного контроля правильности выполнения учетных операций;

Учета и обеспечения сохранности не только документов, но и учетных форм;

Ознакомления или работы с документом только на основании письменной санкции (разрешения) полномочного руководителя, письменного фиксирования всех обращений персонала к документу;

Обязательной росписи руководителей, исполнителей и технического персонала при выполнении любых действий с документом в целях обеспечения персональной ответственности сотрудников фирмы за сохранность носителя и конфиденциальность информации;

Выполнения персоналом введенных в фирме правил работы с конфиденциальными документами, делами и базами данных, обязательными для всех категорий персонала;

Систематических (периодических и разовых) проверок наличия документов у исполнителей, в делах, базах данных, на машинных носителях и т.д., ежедневного контроля сохранности, комплектности, целостности и местонахождения каждого конфиденциального документа;

Коллегиальности процедуры уничтожения документов, дел и баз данных;

Письменного санкционирования полномочным руководителем процедур копирования и тиражирования бумажных и электронных конфиденциальных документов, контроль технологии выполнения этих процедур. Технологическая система обработки и хранения

конфиденциальных документов распространяется не только на управленческую (деловую) документацию, но и конструкторские, технологические, научно-технические и другие аналогичные документы, публикации, нормативные материалы и др., хранящиеся в специальных библиотеках, информационных центрах, ведомственных архивах, документированную информацию, записанную на любом типе носителя информации.