ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо заходів зі зберігання інформаційних ресурсів, наведено технічні характеристики сучасного обладнання для сканування.

У публікації «Структурированное хранилище МФЦ» розповідається про вступ в силу Постанов Уряду РФ №1376 і №1377, які затверджують «Правила функціонування МФЦ», наведені підступи до впровадження структурованого сховища МФЦ.

У публікації «Защита информационных объектов» наведено загальну класифікацію загроз автоматизованій інформаційній системі об'єкту, способи впливу загроз на об'єкти інформаційної безпеки. Розповідається про методи та засоби забезпечення інформаційної безпеки організації (фірми), завдання інформаційної безпеки, вирішення їх за допомогою програмних засобів захисту.

У публікації «Безопасность информационных технологий» розповідається про проблеми забезпечення та причини порушення безпеки комп'ютерних інформаційних систем. Наведено опис математичних моделей систем захисту інформації, а також розглянуто методи і засоби втілення механізмів захисту у існуючих інформаційних системах із можливістю гнучкого управління безпекою в залежності від висунутих вимог, допустимого ризику та оптимального використання ресурсів.

У публікації «Широкоформатные сканеры» наведено стислий опис найбільш популярних моделей широкоформатних сканерів, які запропоновано компанією АКТЕК XXI.

СТРУКТУРИРОВАННОЕ ХРАНИЛИЩЕ МФЦ

Источник: http://www.elar.ru/resheniya/regionalnye_ogv/avtomatizatsiya_gosuslug_i_mfts/strukturirovannoe_khranilishche_mfts/

Введение

Стратегия развития информационного общества направлена на повышение качества взаимодействия граждан, государства и бизнеса. Это снижение административных барьеров и повышение доступности государственных и муниципальных услуг, оптимизация осуществления функций органов исполнительной власти и органов местного самоуправления. Форпостом взаимодействия граждан с государством наряду с «Порталом госуслуг» являются многофункциональные центры (МФЦ).

Вступление в силу в декабре 2012 года Постановлений Правительства РФ №1376 и №1377, утверждающих «Правила функционирования МФЦ» и расширяющих перечень государственных услуг, рекомендованных для предоставления через многофункциональные центры, создало предпосылки для пересмотра подходов к созданию и модернизации автоматизированных информационных систем МФЦ (АИС МФЦ) в части:

- «хранения сведений об истории обращений заявителей в соответствии с требованиями законодательства РФ к программно-аппаратному комплексу информационных систем персональных данных»
- «формирования электронных комплектов документов, содержащих заявления о предоставлении государственной услуги в форме электронного документа, электронные образы документов, необходимых для оказания государственной или муниципальной услуги»
- «поддержка формирования комплекта документов для представления в орган, предоставляющий государственную услугу, в соответствии с требованиями нормативных правовых актов и соглашений о взаимодействии»

Вместе с тем, с учетом определения понятия «Уполномоченного МФЦ» и возможностью (на усмотрение органов региональной власти) наделения его полномочиями «оператора РСМЭВ» актуальной становится задача консолидации документальных фондов, необходимых для предоставления государственных услуг под эгидой МФЦ.

Решение

В целях обеспечения требований, предъявляемых законодательством РФ к организации деятельности МФЦ и обеспечения документационной поддержки предоставления государственных услуг в условиях электронного межведомственного взаимодействия, корпорация ЭЛАР предлагает внедрение апробированного решения «Структурированное хранилище документов и данных МФЦ», которое повысит эффективность деятельности сотрудников МФЦ и снизит затраты на модернизацию используемых АИС.

Программная платформа

Программной платформой решения выступает система управления данными и документами «ЭЛАР-Саперион», развертываемая в инфраструктуре сети МФЦ (региональном ЦОД). Платформа обеспечивает:

- **Структурированное хранение данных и документов** – структура подчинена единому индексу и позволяет создать иерархическую систему хранения разнородной информации (электронные документы, данные и сведения, скан-копии). В т.ч.подписанной ЭП.
- **Инструментарий поиска информации** – широкие возможности по поиску и индексации хранящихся пакетов документов.
- **Сохранность информации** – гарантированное долговременное хранение информации без возможности ее изменения
- **Контроль доступа к информации** – поддержка многоуровневого (до фрагмента документа) контроля из использованием информационных ресурсов
- **Интеграцию** с существующими и проектируемыми системами в части наполнения хранилища, синхронизации справочников и классификаторов и извлечения информации (в т.ч. посредством ВЭБ-сервисов федерального и регионального уровней).

Система сертифицирована в соответствии с требованиями ФСТЭК России по НДВ-4 и разрешена к применению в автоматизированных системах до класса защищенности 1Г включительно и позволяет безопасно обрабатывать персональные данные до категории К1 включительно. Поддерживаются сертифицированные ФСБ средства криптографии и электронной подписи.

Подходы к внедрению структурированного хранилища МФЦ:

Вариант 1

- Создание хранилища пакетов документов по предоставляемым госуслугам. Размещение, хранение и извлечение комплектов документов, содержащих электронные заявления о предоставлении государственной услуги, элетркронные образы, данные и сведения
- Структурированное хранение всех документов, данных и сведений, связанных с фактом предоставления конкретной госуслуги конкуретному лицу
- Поиск пакетов документов сотрудниками МФЦ и вышестоящими организациями на случай спорных ситуаций

Пример для социально-ориентированных госуслуг:

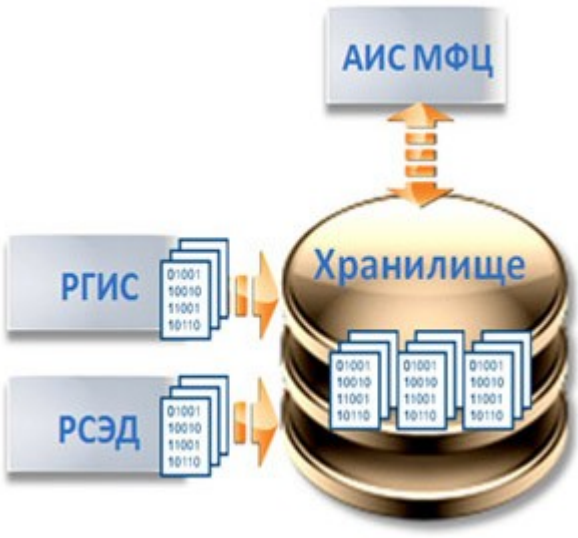
- Пособия по уходу за ребенком
- Предоставление гражданам субсидий на оплату коммунальных услуг
- Предоставление единовременной адресной материальной помощи
- Установление опеки (несовершеннолетние, лица, признанные недееспособными)

Перечень размещаемых в хранилище документов, их источники и форма хранения:

№п/п	Документ	Источник	Форма хранения в электронном виде
1	Паспорт	Личное хранение	Скан-образ
2	Свидетельство о браке	Личное хранение	Скан-образ
3	Распоряжения ОМСУ	Муниципалитет	Скан-образ
4	Справка из образовательного учреждения	Комитет по образованию	Скан-образ
5	Справка о занятости	Служба занятости	Сведения
6	Справка о состоянии здоровья	ЛПУ, ФТЭК	Скан-образ
7	Справка о пособиях	Органы соцзащиты	Сведения

Вариант 2

- Документационное обеспечение деятельности региональной сети МФЦ. Сбор пакетов документов из региональных ГИС и СЭД. Сбор сведений через СМЭВ
- Интеграция с АИС МФЦ, РСМЭВ, РСЭД, локальные СЭД и ГИС организаций поставщиков сведений
- Сбор пакетов документов в электронном виде
- Хранение собранных пакетов
- Поиск документов в хранилище при повторном обращении или конфликтных ситуациях



Пример для госуслуг, связанных с жильем:

- Согласование переустройства или перепланировки жилого помещения
- Перевод жилого помещения в нежилое и нежилого в жилое
- Постановка граждан на учет в качестве нуждающихся в жилье

№№	Документ	Источник	Форма хранения в электронном виде
1	Паспорт	Личное хранение	Скан-образ
2	Свидетельство о браке	Личное хранение	Скан-образ
3	Справка о составе семьи	ЕРЦ	Сведения
4	Справки о платежах	ЕРЦ	Сведения
5	Распоряжения ОМСУ	Муниципалитет	Скан-образ
6	Результаты экспертизы	Служба занятости	Сведения
7	План БТИ	БТИ	Электронный документ
8	Справка о тарифах ЖКХ	Органы соцзащиты	Данные

Вариант 3

- Создание платформы для управления электронными документами данными при предоставлении госуслуг
- Оптимизация межведомственного взаимодействия
- Автоматизация административных регламентов
- Снижение временных затрат для региональных структур при предоставлении сведений и документов
- Уполномоченный МФЦ – оператор РСМЭВ

Пример для госуслуг, связанных с землей и имуществом:

- Предоставление в пользование, аренду или собственность земельных участков
- Выдача градостроительных планов
- Выдача разрешений на строительство

- Выдача разрешений на ввод объектов в эксплуатацию
- Выдача разрешений на установку рекламных конструкций

№№	Документ	Источник	Форма хранения в электронном виде
1	Паспорт	Личное хранение	Скан-образ
2	Градостроительный план ЗУ	Комитет по архитектуре	Скан-образ
3	Отчет о результатах инженерных изысканий	Инженерные службы	Электронный документ
4	Заключение государственной экспертизы ПД	Госэкспертиза	Скан-образ
5	Разрешение на строительство	ОМСУ	Скан-образ
6	Документы, подтверждающие соответствие построенного, реконструированного, отремонтированного ОКС проектной документации	Госэкспертиза	Скан-образ
7	Решение ОМСУ о предоставлении разрешения на условно разрешенный вид использования	ОМСУ	Скан-образ

Преимущества подхода

- Обеспечение требований законодательства (1376-П, 1377-П) в части функционала «АИС МФЦ» и правил функционирования.
- Централизация предоставления госуслуг «в руках» МФЦ – сокращение расходов на предоставление госуслуг.
- Перевод МФЦ на принцип операторского обслуживания (служба «Одного окна») и высвобождение ресурсов региональных ОИВ для профильной деятельности за счет максимальной концентрации необходимых документов и данных в хранилище многофункционального центра.
- Структурированное хранение всех существенных региональных документов и возможность доступа к ним.

ЗАЩИТА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

Источник: http://www.warning.dp.ua/tel28.htm

ВИДЫ УГРОЗ ИНФОРМАЦИОННЫМ ОБЪЕКТАМ

Общая классификация угроз автоматизированной информационной системе объекта выглядит следующим образом:

- Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи.

Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки. При этом используется аппаратура, осуществляющая анализ электромагнитных излучений, возникающих при работе компьютера.

Такой съем информации представляет собой сложную техническую задачу и требует привлечения квалифицированных специалистов. С помощью приемного устройства, выполненного на базе стандартного телевизора, можно перехватывать информацию, выводимую на экраны дисплеев компьютеров с расстояния в тысячу и более метров. Определенные сведения о работе компьютерной системы извлекаются даже в том случае, когда ведется наблюдение за процессом обмена сообщениями без доступа к их содержанию.

- Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой.

Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений. Целостность аппаратуры нарушается при ее повреждении, похищении или незаконном изменении алгоритмов работы.

- Угрозы доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации.

Эта угроза может привести к ненадежности или плохому качеству обслуживания в системе и, следовательно, потенциально будет влиять на достоверность и своевременность доставки платежных документов.

- Угрозы отказа от выполнения трансакций. Возникают в том случае, когда легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность. Оценка уязвимости автоматизированной информационной системы и построение модели воздействий предполагают изучение всех вариантов реализации перечисленных выше угроз и выявление последствий, к которым они приводят.

Угрозы могут быть обусловлены:

– естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);

– человеческими факторами, которые в свою очередь подразделяются на:

-.пассивные угрозы (угрозы, вызванные деятельностью, носящей случайный, неумышленный характер). Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны для воссоединения с семьей и т. п.);

- активные угрозы (угрозы, обусловленные умышленными, преднамеренными действиями людей). Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений, секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); просмотром и передачей различной документации, просмотром «мусора»; подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний, информации (например, в связи с получением другого гражданства по корыстным мотивам);

– человеко-машинными и машинными факторами, подразделяющимися на:

- пассивные угрозы. Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонентов (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.); с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

- активные угрозы. Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение различных видов носителей информации: дискет, описаний, распечаток и других материалов, просмотр вводимых данных, распечаток, просмотр «мусора»); угрозы, реализуемые бесконтактным способом (сбор электромагнитных излучений, перехват сигналов, наводимых в цепях (токопроводящие коммуникации), визуально-оптические способы добычи информации, подслушивание служебных и научно-технических разговоров и т. п.).

Основными типовыми путями утечки информации и несанкционированного доступа к автоматизированным информационным

системам, в том числе через каналы телекоммуникации, являются следующие:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер зашиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- использование «программных ловушек».

Возможными каналами преднамеренного несанкционированного доступа к информации при отсутствии защиты в автоматизированной информационной системе могут быть:

- штатные каналы доступа к информации (терминалы пользователей, средства отображения и документирования информации, носители информации, средства загрузки программного обеспечения, внешние каналы связи) при их незаконном использовании;
- технологические пульты и органы управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами;
- побочное электромагнитное излучение, несущее информацию;
- побочные наводки на цепях электропитания, заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи компьютерной системы.

Способы воздействия угроз на объекты информационной безопасности подразделяются на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование данных в информационных системах;
- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение компьютерных вирусов;

- установку программных и аппаратных закладных устройств;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других оригинальных носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты информации;
- воздействие на персонал;
- поставку «зараженных» компонентов автоматизированных информационных систем.

Радиоэлектронными способами являются:

- перехват информации в технических каналах ее возможной утечки;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Угрозы безопасности программного обеспечения. Обеспечение безопасности автоматизированных информационных систем зависит от безопасности используемого в них программного обеспечения и, в частности, следующих видов программ:

- обычных программ пользователей;
- специальных программ, рассчитанных на нарушение безопасности системы;
- разнообразных системных утилит и коммерческих прикладных программ, которые отличаются высоким профессиональным уровнем разработки и тем не менее могут содержать отдельные недоработки, позволяющие захватчикам атаковать системы.

Программы могут порождать проблемы двух типов: во-первых, могут перехватывать и модифицировать данные в результате действий пользователя, который к этим данным не имеет доступа, и, во-вторых, используя упущения в защите компьютерных систем, могут или обеспечивать доступ к системе пользователям, не имеющим на это права, или блокировать доступ к системе законных пользователей.

Чем выше уровень подготовки программиста, тем более неявными (даже для него) становятся допускаемые им ошибки и тем более тщательно и

надежно он способен скрыть умышленные механизмы, разработанные для нарушения безопасности системы.

Целью атаки могут быть и сами программы по следующим причинам:

- В современном мире программы могут быть товаром, приносящим немалую прибыль, особенно тому, кто первым начнет тиражировать программу в коммерческих целях и оформит авторские права на нее.
- Программы могут становиться также объектом атаки, имеющей целью модифицировать эти программы некоторым образом, что позволило бы в будущем провести атаку на другие объекты системы. Особенно часто объектом атак такого рода становятся программы, реализующие функции защиты системы.

Рассмотрим несколько типов программ и приемы, которые наиболее часто используются для атак программ и данных. Эти приемы обозначаются единым термином — «программные ловушки». К ним относятся «программные люки», «троянские кони», «логические бомбы», атаки «салями», скрытые каналы, отказы в обслуживании и компьютерные вирусы.

Люки в программах. Использование люков для проникновения в программу — один из простых и часто используемых способов нарушения безопасности автоматизированных информационных систем.

Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности, выход в привилегированный режим).

Люки чаще всего являются результатом забывчивости разработчиков. В качестве люка может быть использован временный механизм прямого доступа к частям продукта, созданный для облегчения процесса отладки и не удаленный по ее окончании. Люки могут образовываться также в результате часто практикуемой технологии разработки программных продуктов «сверху вниз»: в их роли будут выступать оставленные по каким-либо причинам в готовом продукте «заглушки» — группы команд, имитирующие или просто обозначающие место подсоединения будущих подпрограмм.

Наконец, еще одним распространенным источником люков является так называемый «неопределенный ввод» — ввод «бессмысленной» информации, абракадабры в ответ на запросы системы. Реакция недостаточно хорошо написанной программы на неопределенный ввод может быть, в лучшем случае, непредсказуемой (когда при повторном вводе той же неверной команды программа реагирует каждый раз по-разному); гораздо хуже, если программа в результате одинакового «неопределенного» ввода выполняет некоторые повторяющиеся действия, — это дает возможность потенциальному захватчику планировать свои действия по нарушению безопасности.

Неопределенный ввод — частная реализация прерывания. То есть в общем случае захватчик может умышленно пойти на создание в системе некоторой нестандартной ситуации, которая бы позволила ему выполнить необходимые действия. Например, он может искусственно вызвать аварийное завершение программы, работающей в привилегированном режиме, с тем, чтобы перехватить управление, оставшись в этом привилегированном режиме.

Борьба с возможностью прерывания, в конечном счете, выливается в необходимость предусмотреть при разработке программ комплекса механизмов, образующих так называемую «защиту от дурака». Смысл этой защиты состоит в том, чтобы гарантированно отсекать всякую вероятность обработки неопределенного ввода и разного рода нестандартных ситуаций (в частности, ошибок) и тем самым не допускать нарушения безопасности компьютерной системы даже в случае некорректной работы с программой.

Таким образом, люк (или люки) может присутствовать в программе ввиду того, что программист:

- забыл удалить его;
- умышленно оставил его в программе для обеспечения тестирования или выполнения оставшейся части отладки;
- умышленно оставил его в программе в интересах облегчения окончательной сборки конечного программного продукта;
- умышленно оставил его в программе с тем, чтобы иметь скрытое средство доступа к программе уже после того, как она вошла в состав конечного продукта.

Люк — первый шаг к атаке системы, возможность проникнуть в компьютерную систему в обход механизмов защиты.

«Троянские кони». Существуют программы, реализующие, помимо функций, описанных в документации, и некоторые другие функции, в документации не описанные. Такие программы называются «троянскими конями».

Вероятность обнаружения «троянского коня» тем выше, чем очевиднее результаты его действий (например, удаление файлов или изменение их защиты). Более сложные «троянские кони» могут маскировать следы своей деятельности (например, возвращать защиту файлов в исходное состояние).

«Логические бомбы». «Логической бомбой» обычно называют программу или даже участок кода в программе, реализующий некоторую функцию при выполнении определенного условия. Этим условием может быть, например, наступление определенной даты или обнаружение файла с определенным именем.

«Взрываясь», «логическая бомба» реализует функцию, неожиданную и, как правило, нежелательную для пользователя (например, удаляет некоторые данные или разрушает некоторые системные структуры). «Логическая бомба» является одним из излюбленных способов мести программистов компаниям, которые их уволили или чем-либо обидели.

Атака «салями». Атака «салями» превратилась в настоящий бич банковских компьютерных систем. В банковских системах ежедневно производятся тысячи операций, связанных с безналичными расчетами, переводами сумм, отчислениями и т. д.

При обработке счетов используются целые единицы (рубли, центы), а при исчислении процентов нередко получаются дробные суммы. Обычно величины, превышающие половину рубля (цента), округляются до целого рубля (цента), а величины менее половины рубля (цента) просто отбрасываются. При атаке «салями» эти несущественные величины не удаляются, а постепенно накапливаются на некоем специальном счете.

Как свидетельствует практика, сумма, составленная буквально из ничего, за пару лет эксплуатации «хитрой» программы в среднем по размеру банке может исчисляться тысячами долларов. Атаки «салями» достаточно трудно распознаются, если злоумышленник не начинает накапливать на одном счете большие суммы.

Скрытые каналы. Под скрытыми каналами подразумеваются программы, передающие информацию лицам, которые в обычных условиях эту информацию получать не должны.

В тех системах, где ведется обработка критичной информации, программист не должен иметь доступа к обрабатываемым программой данным после начала эксплуатации этой программы.

Из факта обладания некоторой служебной информацией можно извлечь немалую выгоду, хотя бы элементарно продав эту информацию (например, список клиентов) конкурирующей фирме. Достаточно квалифицированный программист всегда может найти способ скрытой передачи информации; при этом программа, предназначенная для создания самых безобидных отчетов, может быть немного сложнее, чем того требует задача.

Для скрытой передачи информации можно с успехом использовать различные элементы формата «безобидных» отчетов, например разную длину строк, пропуски между строками, наличие или отсутствие служебных заголовков, управляемый вывод незначащих цифр в выводимых величинах, количество пробелов или других символов в определенных местах отчета и т. д.

Если захватчик имеет возможность доступа к компьютеру во время работы интересующей его программы, скрытым каналом может стать пересылка критичной информации в специально созданный в оперативной памяти компьютера массив данных.

Скрытые каналы наиболее применимы в ситуациях, когда захватчика интересует даже не содержание информации, а, допустим, факт ее наличия (например, наличие в банке расчетного счета с определенным номером).

Отказ в обслуживании. Большинство методов нарушения безопасности направлено на то, чтобы получить доступ к данным, не допускаемый системой в нормальных условиях. Однако не менее интересным для захватчиков является доступ к управлению самой компьютерной системой или изменение ее качественных характеристик, например, получить

некоторый ресурс (процессор, устройство ввода-вывода) в монопольное использование или спровоцировать ситуацию клинча для нескольких процессов.

Это может потребоваться для того, чтобы явно использовать компьютерную систему в своих целях (хотя бы для бесплатного решения своих задач) либо просто заблокировать систему, сделав ее недоступной другим пользователям. Такой вид нарушения безопасности системы называется «отказом в обслуживании» или «отказом от пользы». «Отказ в обслуживании» чрезвычайно опасен для систем реального времени — систем, управляющих некоторыми технологическими процессами, осуществляющих различного рода синхронизацию и т. д.

Компьютерные вирусы. Компьютерные вирусы являются квинтэссенцией всевозможных методов нарушения безопасности. Одним из самых частых и излюбленных способов распространения вирусов является метод «троянского коня». От «логической бомбы» вирусы отличаются только возможностью размножаться и обеспечивать свой запуск, так что многие вирусы можно считать особой формой «логических бомб».

Для атаки системы вирусы активно используют разного рода «люки». Вирусы могут реализовывать самые разнообразные пакости, в том числе и атаку «салями». Кроме того, успех атаки одного вида часто способствует снижению «иммунитета» системы, создает благоприятную среду для успеха атак других видов. Захватчики это знают и активно используют данное обстоятельство.

Разумеется, в чистом виде описанные выше приемы встречаются достаточно редко. Гораздо чаще в ходе атаки используются отдельные элементы разных приемов.

Угрозы информации в компьютерных сетях. Сети компьютеров имеют много преимуществ перед совокупностью отдельно работающих компьютеров, в их числе можно отметить: разделение ресурсов системы, повышение надежности функционирования системы, распределение загрузки среди узлов сети и расширяемость за счет добавления новых узлов.

Вместе с тем при использовании компьютерных сетей возникают серьезные проблемы обеспечения информационной безопасности. Можно отметить следующие из них.

Разделение совместно используемых ресурсов. В силу совместного использования большого количества ресурсов различными пользователями сети, возможно, находящимися на большом расстоянии друг от друга, сильно повышается риск несанкционированного доступа, так как в сети его можно осуществить проще и незаметнее.

Расширение зоны контроля. Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости.

Комбинация различных программно-аппаратных средств. Соединение нескольких систем в сеть увеличивает уязвимость всей системы в целом, поскольку каждая информационная система настроена на выполнение своих

специфических требований безопасности, которые могут оказаться несовместимыми с требованиями на других системах.

Неизвестный параметр. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно, так как один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда можно точно определить, сколько пользователей имеют доступ к определенному узлу сети и кто они.

Множество точек атаки. В сетях один и тот же набор данных или сообщение может передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки.

Сложность управления и контроля доступа к системе. Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу — с помощью сети из удаленных точек.

В этом случае идентификация нарушителя может оказаться очень сложной. Кроме того, время атаки может оказаться слишком малым для принятия адекватных мер.

С одной стороны, сеть — это единая система с едиными правилами обработки информации, а с другой — совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. Поэтому, с учетом двойственности характера сети, атака на сеть может осуществляться с двух уровней: верхнего и нижнего (возможна и их комбинация).

При верхнем уровне атаки на сеть злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий. При нижнем уровне атаки на сеть злоумышленник использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом.

Нарушение потока сообщений может привести к утечке информации и даже потере контроля над сетью.

Различают пассивные и активные угрозы нижнего уровня, специфические для сетей.

Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) – это просмотр и/или запись данных, передаваемых по линиям связи. К ним относятся:

- просмотр сообщения;
- анализ графика — злоумышленник может просматривать заголовки пакетов, циркулирующих в сети, и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности, длина сообщения, объем трафика и т. д.).

Активные угрозы (нарушение целостности или доступности ресурсов и компонентов сети) — несанкционированное использование устройств, имеющих доступ к сети для изменения отдельных сообщений или потока сообщений. К ним относятся:

- отказ служб передачи сообщений — злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;
- «маскарад» — злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;
- внедрение сетевых вирусов — передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;
- модификация потока сообщений — злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Угрозы коммерческой информации. В условиях информатизации особую опасность представляют также такие способы несанкционированного доступа к конфиденциальной информации, как копирование, подделка, уничтожение.

Копирование. При несанкционированном доступе к конфиденциальной информации копируют: документы, содержащие интересующую злоумышленника информацию; технические носители; информацию, обрабатываемую в автоматизированных информационных системах. Используются следующие способы копирования: светокопирование, фотокопирование, термокопирование, ксерокопирование и электронное копирование.

Подделка. В условиях конкуренции подделка, модификация и имитация приобретают большие масштабы. Злоумышленники подделывают доверительные документы, позволяющие получить определенную информацию, письма, счета, бухгалтерскую и финансовую документацию; подделывают ключи, пропуска, пароли, шифры и т. п. В автоматизированных информационных системах к подделке относят, в частности, такие злонамеренные действия, как фальсификация (абонент-получатель подделывает полученное сообщение, выдавая его за действительное в своих интересах), маскировка (абонент-отправитель маскируется под другого абонента с целью получения им охраняемых сведений).

Уничтожение. Особую опасность представляет уничтожение информации в автоматизированных базах данных и базах знаний. Уничтожается информация на магнитных носителях с помощью компактных магнитов и программным путем («логические бомбы»). Значительное место в преступлениях против автоматизированных информационных систем занимают саботаж, взрывы, разрушения, вывод из строя соединительных кабелей, систем кондиционирования.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ФИРМЫ).

Методами обеспечения защиты информации являются следующие: препятствие, управление доступом, маскировка, регламентация, принуждение и побуждение.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Управление доступом — метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы организации (фирмы). Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
- аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка — метод защиты информации в автоматизированной информационной системе путем ее криптографического закрытия.

Регламентация — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение — такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — такой метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности организации (фирмы) реализуются на практике применением различных механизмов защиты, для создания которых используются следующие основные средства: физические, аппаратные, программные, аппаратно-программные, криптографические, организационные, законодательные и морально-этические.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной

информационной системы предприятия и реализуются в виде автономных устройств и систем.

Наряду с традиционными механическими системами при доминирующем участии человека разрабатываются и внедряются универсальные автоматизированные электронные системы физической защиты, предназначенные для охраны территорий, охраны помещений, организации пропускного режима, организации наблюдения; системы пожарной сигнализации; системы предотвращения хищения носителей.

Элементную базу таких систем составляют различные датчики, сигналы от которых обрабатываются микропроцессорами, электронные интеллектуальные ключи, устройства определения биометрических характеристик человека и т. д.

Для организации охраны оборудования, входящего в состав автоматизированной информационной системы предприятия, и перемещаемых носителей информации (дискеты, магнитные ленты, распечатки) используются:

- различные замки (механические, с кодовым набором, с управлением от микропроцессора, радиоуправляемые), которые устанавливают на входные двери, ставни, сейфы, шкафы, устройства и блоки системы;
- микровыключатели, фиксирующие открывание или закрывание дверей и окон;
- инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку телевизионных антенн;
- специальные наклейки из фольги, которые наклеиваются на все документы, приборы, узлы и блоки системы для предотвращения их выноса из помещения. При любой попытке вынести за пределы помещения предмет с наклейкой специальная установка (аналог детектора металлических объектов), размещенная около выхода, подает сигнал тревоги;
- специальные сейфы и металлические шкафы для установки в них отдельных элементов автоматизированной информационной системы (файл-сервер, принтер и т. п.) и перемещаемых носителей информации.

Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия. При этом:

- экранирование рабочих помещений, где установлены компоненты автоматизированной информационной системы, осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установкой загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или из специальной пластмассы листов;
- для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем;
- все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой;
- на вентиляционных каналах монтируют предельные магнитные ловушки, препятствующие распространению радиоволн.

Для защиты от наводок на электрические цепи узлов и блоков автоматизированной информационной системы используют:

- экранированный кабель для внутристоечного, внутриблочного, межблочного и наружного монтажа;
- экранированные эластичные соединители (разъемы), сетевые фильтры подавления электромагнитных излучений;
- провода, наконечники, дроссели, конденсаторы и другие помехоподавляющие радио- и электроизделия;
- на водопроводных, отопительных, газовых и других металлических трубах помещают разделительные диэлектрические вставки, которые осуществляют разрыв электромагнитной цепи.

Для контроля электропитания используются электронные отслеживатели – устройства, которые устанавливаются в местах ввода сети переменного напряжения. Если шнур питания перерезан, оборван или перегорел, кодированное послание включает сигнал тревоги или активирует телевизионную камеру для последующей записи событий.
Для обнаружения внедренных «жучков» наиболее эффективным считается рентгеновское обследование. Однако реализация этого метода связана с большими организационными и техническими трудностями.
Применение специальных генераторов шумов для защиты от хищения информации с компьютеров путем съема ее излучений с экранов дисплеев оказывает неблагоприятное воздействие на организм человека, что приводит к быстрому облысению, снижению аппетита, головным болям, тошноте. Именно поэтому они достаточно редко применяются на практике.

Аппаратные средства защиты – это различные электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками.

Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т. д.

Основные функции аппаратных средств защиты:

- запрещение несанкционированного (неавторизованного) внешнего доступа (удаленного пользователя, злоумышленника) к работающей автоматизированной информационной системе;
- запрещение несанкционированного внутреннего доступа к отдельным файлам или базам данных информационной системы, возможного в результате случайных или умышленных действий обслуживающего персонала;
- защита активных и пассивных (архивных) файлов и баз данных, связанная с необслуживанием или отключением автоматизированной информационной системы;
- защита целостности программного обеспечения.

Эти задачи реализуются аппаратными средствами защиты информации с использованием метода управления доступом (идентификация,

аутентификация и проверка полномочий субъектов системы, регистрация и реагирование).

Для работы с особо ценной информацией организации (фирмы) производители компьютеров могут изготавливать индивидуальные диски с уникальными физическими характеристиками, не позволяющими считывать информацию. При этом стоимость компьютера может возрасти в несколько раз.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, включающих разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т. п.);
- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;
- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);
- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;
- защита информации от компьютерных вирусов;
- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;
- стирание остаточной конфиденциальной информации на магнитных дисках, выдача протоколов о результатах стирания;
- обеспечение целостности информации путем введения избыточности данных;
- автоматический контроль над работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

В настоящее время ряд операционных систем изначально содержит встроенные средства блокировки «повторного использования». Для других

типов операционных систем существует достаточно много коммерческих программ, не говоря уже о специальных пакетах безопасности, реализующих аналогичные функции.

Применение избыточных данных направлено на предотвращение появления в данных случайных ошибок и выявление неавторизованных модификаций. Это может быть применение контрольных сумм, контроль данных на чет-нечет, помехоустойчивое кодирование и т. д.

Часто практикуется хранение в некотором защищенном месте системы сигнатур важных объектов системы. Например, для файла в качестве сигнатуры может быть использовано сочетание байта защиты файла с его именем, длиной и датой последней модификации. При каждом обращении к файлу или в случае возникновения подозрений текущие характеристики файла сравниваются с эталоном.

Свойство ревизуемости системы контроля доступа означает возможность реконструкции событий или процедур. Средства обеспечения ревизуемости должны выяснить, что же фактически случилось. Здесь речь идет о документировании исполняемых процедур, ведении журналов регистрации, а также о применении четких и недвусмысленных методов идентификации и проверки.

Следует отметить, что задачу контроля доступа при одновременном обеспечении целостности ресурсов надежно решает только шифрование информации.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Источник: http://www.warning.dp.ua/comp7.htm

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Понятие системности

Понятие системности заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации объединяются в единый целостный механизм - систему защиты.

К сожалению необходимость комплексного обеспечения безопасности информационных технологий пока не находит должного понимания у пользователей современных ИС. В то же время построение систем защиты информации не ограничивается простым выбором тех или иных средств

защиты. Для создания таких систем необходимо иметь определенные теоретические знания, а именно:

- что представляет собой защищенная информационная система,
- что такое система защиты информации и какие требования предъявляются к ней,
- какие существуют угрозы и причины нарушения безопасности информационных технологий,
- какие функции защиты и каким образом должны быть реализованы, как они противодействуют угрозам и устраняют причины нарушения безопасности,
- как построить комплексную систему защиты информации,
- как достичь высокого уровня безопасности при приемлемых затратах на средства защиты информации и многое, многое другое..

Учитывая, что современная нормативно-методическая база в этой области не дает полного представления о том, как организовать защиту информации, часто приходится действовать на свой страх и риск, поэтому с целью уменьшения вероятности принятия ошибочных решений, хотелось бы сформировать у читателя целостное представление о проблемах защиты информации и путях их решения.

Существующие публикации на эту тему в основном ограничиваются перечислением угроз и возможностей конкретных средств защиты информации. В книге представлен полный спектр вопросов о практическом создании защищенных информационных систем.

Почему это важно

Вопросы безопасности информации - важная часть процесса внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенных ИС, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Реализация угроз несанкционированного использования информации наносит сейчас гораздо больший ущерб, чем, например, "случайные" пожары в помещениях или физическое воздействие на сотрудников. Однако затраты на построение системы защиты информации еще пока несоизмеримо малы по сравнению с затратами на защиту от грабителей или на противопожарную защиту.

К тому же в современном бизнесе наблюдается постепенный переход от чисто физических методов воздействия на конкурентов к более интеллектуальным, в том числе с использованием новейших средств и способов добывания информации.

Что хотелось сказать

На страницах книги в популярной форме изложены причины нарушения безопасности компьютерных систем, приведено описание

математических моделей систем защиты информации, а также рассмотрены методы и средства внедрения механизмов защиты в существующие информационные системы с возможностью гибкого управления безопасностью в зависимости от выдвигаемых требований, допустимого риска и оптимального расхода ресурсов.

Автор старается осветить ряд вопросов, связанных с обеспечением безопасности информационных технологий, а также стремится сформировать целостное представление о путях создания систем защиты информации.

Разумеется, данная публикация не претендует на окончательное разрешение всех проблем информационной безопасности, но, как надеется автор, предложенный материал прояснит ряд вопросов из этой области знаний и позволит решить многие практические задачи.

Возможно, читатель не откроет для себя ничего принципиально нового, пролистав эту книгу, однако системный подход в изложении материала позволит по-новому, с разных сторон взглянуть на проблемы обеспечения безопасности современных информационных технологий.

Методика систематизации и представления экспертных знаний о требованиях, предъявляемых к комплексным системам защиты информации (КСЗИ)

Существующие подходы и методики оценки уровня защиты отражают показатели отдельных элементов КСЗИ, однако, достаточно полных оценок с учетом логического и функционального объединения требований к КСЗИ в единый комплекс мероприятий по созданию КСЗИ ИССН до сих пор не проводилось. На основе анализа литературы, нормативных документов, статей и других материалов, а также с учетом практических наработок, предлагается следующая методика систематизации и представления экспертных знаний о требованиях, предъявляемых к КСЗИ.

Модель КСЗИ представлена в виде следующих основных блоков показателей:

Блок показателей "ОСНОВЫ";

Блок показателей "НАПРАВЛЕНИЯ";

Блок показателей "ЭТАПЫ";

(рис. 1).

Проведенный анализ подходов к созданию КСЗИ ИССН показал, что ОСНОВОЙ или составными частями практически любой системы, в том числе и системы защиты информации, являются:

- законодательная, нормативно-правовая и научная база;
- структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
- организационно-технические и режимные меры (политика информационной безопасности);
- программно-технические способы и средства.

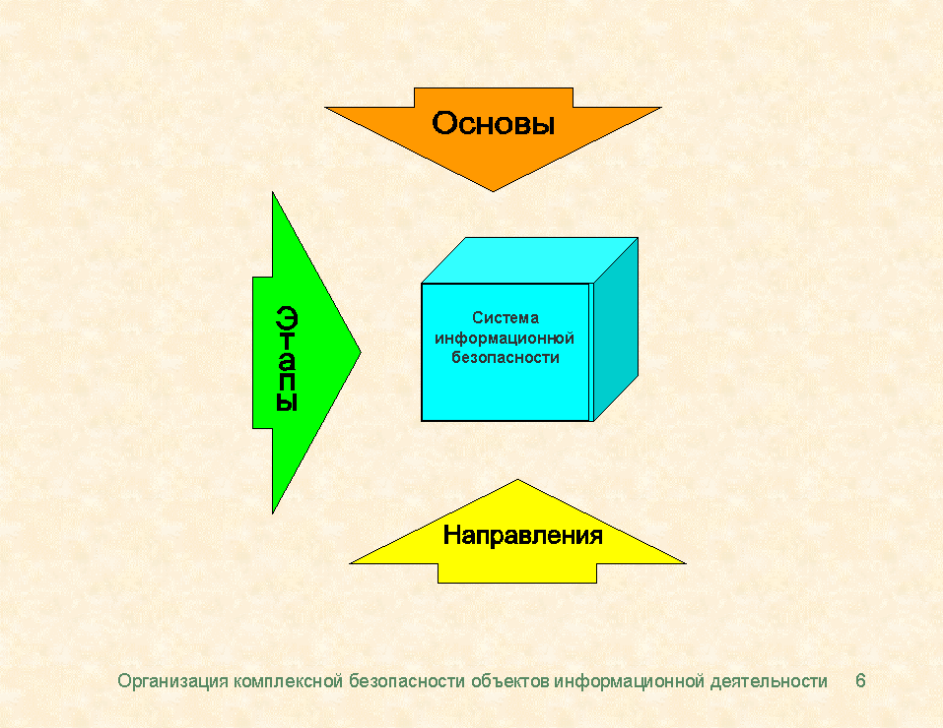


Рис. 1 – Модель комплексной системы защиты информации

Обозначим указанные показатели КСЗИ следующим образом:

О1 - Качество нормативно-правовой и научной базы;

О2 - Полнота структуры и задач органов, обеспечивающих защиту;

О3 - Качество организационных мер и методов защиты информации (политика безопасности);

О4 - Качество программно-технических способов и средств защиты.

Каждый из перечисленных показателей блока "ОСНОВЫ" описывается частными показателями Oi-n, которые характеризуют конкретную ИССН.

Примером частных показателей блока "ОСНОВЫ" могут быть:

- правовые вопросы защиты массивов информации от искажений и установления юридической ответственности по обеспечению сохранности информации (показатель Oi-1);

- юридические и технические вопросы защиты хранящейся информации от несанкционированного доступа к ней, исключающие возможность неправомерного использования ее (показатель Oi-2);

- юридически закрепленные нормы и методы защиты программного обеспечения (Oi-3);

- мероприятия по приданию юридической силы электронным документам, и формирование юридических норм для лиц, ответственных за качество таких документов (показатель Oi-4).

Проведенный анализ существующих способов и методов защиты информации позволяет выделить следующие основные сложившиеся на практике НАПРАВЛЕНИЯ создания и оценки КСЗИ (рис. 2).

Рис. 2 – Блок показателей Основы информационной безопасности

Обозначим показатели:

H1 - уровень защиты объектов ИССН;

H2 - уровень защиты процессов, процедур и программ обработки информации;

H3 - уровень защиты каналов связи;

H4 - уровень подавления побочных электромагнитных излучений;

H5 - качество управления системой защиты.

Совершенно очевидно, что каждый из показателей блока "НАПРАВЛЕНИЯ" должен быть детализирован в зависимости от структуры ИССН частными показателями. Число возможных составных показателей, входящих в блок "НАПРАВЛЕНИЯ" обозначим Hj (при j от 1 до n). Каждый из перечисленных показателей блока "НАПРАВЛЕНИЯ" описывается частными показателями Hi-n , которые характеризуют конкретную ИССН.

Направления информационной безопасности в графическом виде представлены на рис. 3.

В настоящее время рассматривают различные этапы построения КСЗИ, все они достаточно эффективны и позволяют решать поставленные задачи. На основе проведенного анализа предлагается рассмотрение следующих этапов создания КСЗИ, подлежащих оценке:

Определение информационных и технических ресурсов, а также объектов ИС подлежащих защите;

Выявление потенциально возможных угроз и каналов утечки информации;

Проведение оценки уязвимости и рисков информации (ресурсов ИС) при имеющемся множестве угроз и каналов утечки;

Определение требований к системе защиты информации;

Осуществление выбора средств защиты информации и их характеристик;

Внедрение и организация использования выбранных мер, способов и средств защиты.

Осуществление контроля целостности и управление системой защиты.

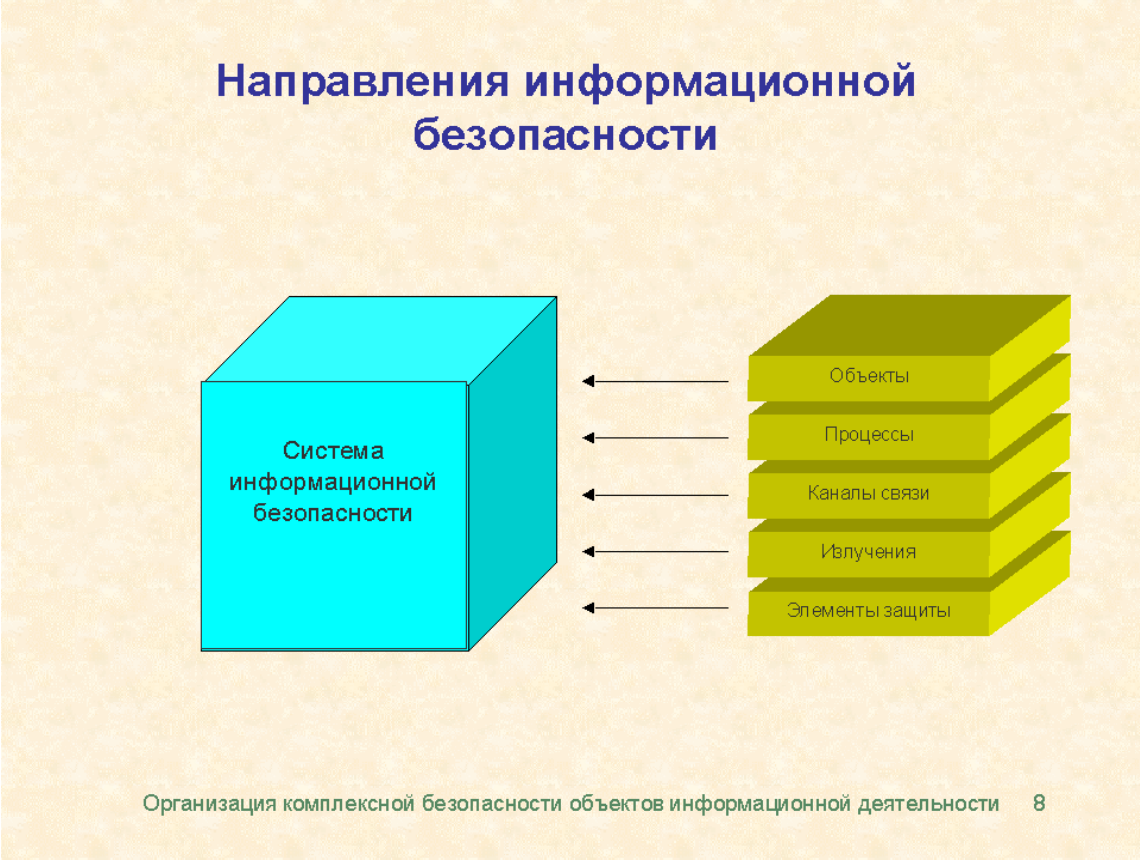


Рис. 3 – Блок показателей направления информационной безопасности

Представим указанные этапы в виде показателей:

М1 - полнота определения информации, подлежащей защите;

М2 - полнота выявления множества потенциально возможных угроз и каналов утечки информации;

М3 - качество проведения оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

М4 - качество определения требований к системе защиты;

М5 - качество выбора средств защиты информации и их характеристик;

М6 - уровень внедрения и организация использования выбранных мер, способов и средств защиты;

М7 - качество контроля целостности и управление системой защиты.

Этапы могут быть разбиты на более детальные пункты (шаги). Общее число показателей "ЭТАПЫ" обозначим Mk (при k=от 1 до n). Каждый из перечисленных показателей блока "ЭТАПЫ" описывается частными показателями Mi-n, которые характеризуют конкретную ИССН (рис. 3.6).

Примерами частных показателей блока "ЭТАПЫ", а именно показателя, определяющего требования к системе защиты (М4), могут быть следующие:

- качество определения требований к политике безопасности (М4-1);
- качество определения требований к меткам безопасности (М4-2);
- качество определения требований к идентификации и аутентификации (М4-3);
- качество определения требований к регистрации и учету (М4-4);
- качество определения требований к контролю корректности функционирования средств защиты (М4-5).

Этапы формирования информационной безопасности наглядно показаны на рис. 4. КСЗИ заключается в логическом объединении показателей блоков "ОСНОВЫ", "НАПРАВЛЕНИЯ" и "ЭТАПЫ" в МАТРИЦУ ЗНАНИЙ, состоящую из К элементов.

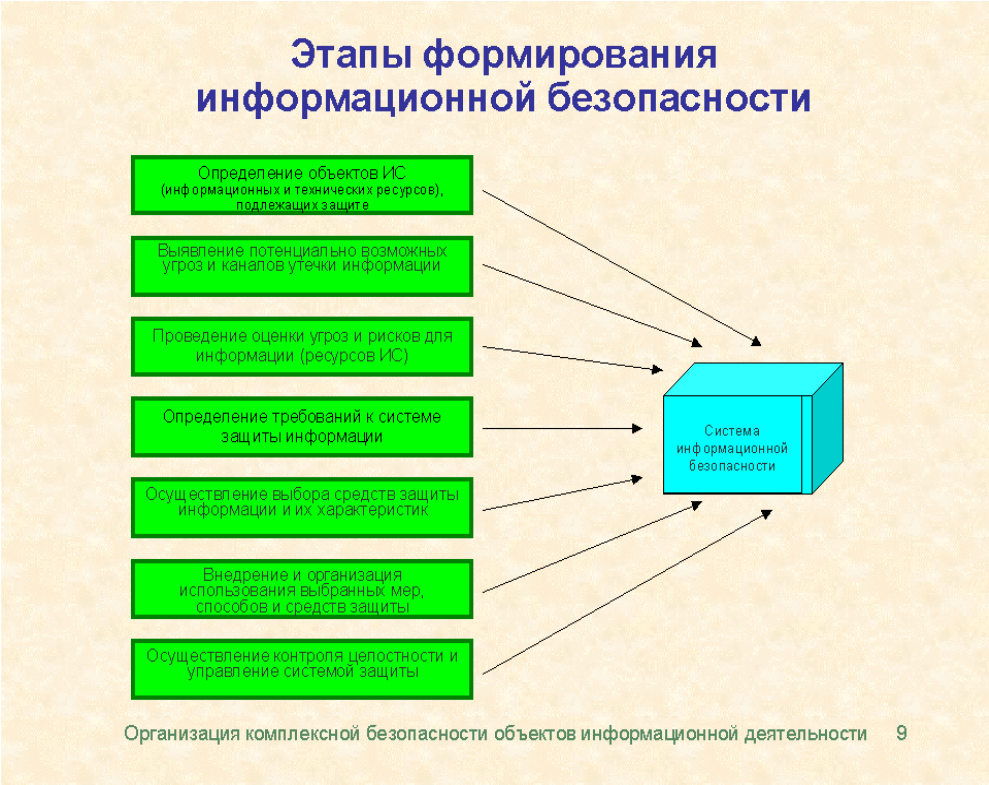


Рис. 4 – Этапы формирования информационной безопасности

В общем случае количество элементов МАТРИЦЫ ЗНАНИЙ может быть определено из соотношения:

K=Oi*Hj*Mk,

где К - количество элементов матрицы;

Oi - количество составляющих блока "ОСНОВЫ";

Hj - количество составляющих блока "НАПРАВЛЕНИЯ"

Mk - количество составляющих блока "ЭТАПЫ".

На основе проведенного выше анализа в данном варианте (при условии, что Oi=4, Hj=5, Mk=7) общее количество элементов матрицы знаний составляет

K=4*5*7=140.

Следует обратить внимание на содержание обозначения каждого из элементов матрицы.

Первое знакоместо обозначает номер показателя "ЭТАПЫ", второе знакоместо - номер показателя "НАПРАВЛЕНИЯ", а третье знакоместо - номер показателя "ОСНОВЫ".

Пример, элемента матрицы 321, который формируется с учетом следующих показателей:

300 - Проведение оценки уязвимости и рисков (показатель № 3 блока "ЭТАПЫ");

020 - Защита процессов и программ (показатель № 2 блока "НАПРАВЛЕНИЯ");

001 - Нормативная база (показатель № 1 блока "ОСНОВЫ").

Для примера рассмотрим содержание элементов матрицы № 321, 322, 323, 324, которые объединяют показатель № 3 блока "ЭТАПЫ", показатель № 2 блока "НАПРАВЛЕНИЯ" и показатели № 1, 2, 3, 4 блока "ОСНОВЫ".

Элемент со значением индексов 321 характеризует, насколько полно отражены в законодательных, нормативных и методических документах вопросы, определяющие порядок проведения оценки уязвимости и рисков для информации, используемой в процессах и программах конкретной ИССН;

Элемент со значением индексов 322 определяет, имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИССН;

Элемент со значением индексов 323 рассматривает, определены ли режимные меры, обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИССН;

Элемент со значением индексов 3.2.4 определяет, применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИССН.

Это только четыре вопроса из ста сорока (для данного варианта), но ответы на них уже позволяют сформировать некое представление о состоянии дел по защите информации в конкретной ИССН.

В нашем случае для матрицы знаний формируется 140 вопросов (по числу ее элементов). Содержание каждого из элементов матрицы описывает взаимосвязь составляющих в создаваемой КСЗИ. Сформулировав ответы на все вопросы можно составить полное представление о КСЗИ и оценить достигнутый уровень защиты. Вариант разработанного автором полного перечня вопросов приведен в приложении А.

Кроме того, использование матрицы позволяет решать комплекс вопросов создания и оценки КСЗИ путем анализа различных групп элементов матрицы, в зависимости от решаемых задач. Например отдельно можно оценить качество нормативной базы КСЗИ, или защищенность каналов связи, или качество мероприятий по выявлению каналов утечки информации и т.д.

Показатели уровней защиты КСЗИ предлагается определять методом экспертных оценок, используя положения теории нечеткой логики и нечетких утверждений. Величина показателей каждого из элементов матрицы определяется на основе использования соответствующих функций принадлежности.

ШИРОКОФОРМАТНЫЕ СКАНЕРЫ

Источник: http://www.storage-systems.ru/scanners/largescanners/

Широкоформатные сканеры используются для сканирования карт, чертежей и других документов большого формата, обеспечивая высочайшее разрешение и точную цветопередачу даже при компактных размерах.

Всю самую свежую и полную информацию о широкоформатных сканерах на английском языке вы сможете найти на сайте производителя.

Краткие описания наиболее популярных моделей широкоформатных сканеров, предлагаемых компанией АКТЕК XXI, представлены ниже:

Зойчель Омнискан 10000 A0

Широкоформатный цветной книжный сканер для библиотек и архивов

Ежегодно тысячи и тысячи ценнейших книг, карт и документов в библиотеках и архивах приходят в негодность, проходя через множество людских рук, разрушаются от воздействия неблагоприятных условий хранения и использования. С исчезновением этих работ, мы навсегда теряем уникальную информацию, содержащуюся в них.

Широкоформатный цветной планетарный сканер формата A0 Zeutschel Omniscan 10000 A0 специально разработан для библиотек и архивов. Он

предназначен для сканирования книг, газет и документов большого формата (карт, чертежей и т.п.), в том числе ветхих и поврежденных. Широкоформатный сканер Omniscan 10000 A0 позволяет значительно повысить сохранность документов в библиотеках и архивах, благодаря очень деликатному обращению с оригиналами. В системе освещения отсутствует ультрафиолетовая компонента излучения, которая может повредить оригинал. Широкоформатный сканер Omniscan 10000 A0 позволяет сканировать документы формата до 871x1220 мм за несколько секунд. Широкоформатный сканер Omniscan 10000 A0 удачно сочетает эргономичный дизайн с высочайшими стандартами оцифровки уникальных и бесценных документов.

Преимущества широкоформатного сканера Zeutschel Omniscan 10000 A0

- Очень низкое воздействие излучения на оригинал
- Высокая производительность, в том числе благодаря функции ограничения области сканирования
- Скорость сканирования настраивается под ваши потребности
- Точное воспроизведение цветов оригинала
- Освещение активируется только на время сканирования
- Отсутствует ультрафиолетовая составляющая излучения
- Отсутствует тепловое воздействие излучения на оператора и оригинал
- Отсутствуют блики при сканировании глянцевых документов
- Очень удобная работа с прижимным стеклом благодаря эргономичной книжной колыбели Zeutschel
- Возможность работы без прижимного стекла
- Простое и эффективное программное обеспечение

Технические характеристики сканера Zeutschel Omniscan 10000 A0

Описание	Высокопроизводительная широкоформатный планетарный сканер (сканирующая система) для книг, газет и документов большого формата (чертежей, карт, документов)
Размер оригиналов	871x1220 мм (>DIN A0/D)
Стол сканера	Широкий выбор столов, стол с верхней подсветкой AT-0, книжная колыбель OT 180 H/A0, колыбель для ветхих книг OT 90, стол с подсветкой (возможно со стеклянной пластиной), стол для газет (смотрите отдельную брошюру по столам серии OT)
Сканирующая головка	Высокопроизводительная сканирующая головка: 3x21000x14800 пикселей, высокоточные сканирующие линзы без искажений, глубина фокуса 50 мм, 36-битный цвет
Максимальное разрешение сканирования	400 dpi (до 600 dpi по дополнительному запросу)
Скорость сканирования	40 секунд при 400 dpi
Интерфейс широкоформатного сканера	SCSI-3 Ultra Wide
Формат изображений	Все стандартные форматы изображений: несжатый TIFF, TIFF G4, JPEG, многостраничный TIFF, PDF, BMP, PCX
Прикладное ПО	OS 11 для высокой производительности со всеми стандартными инструментами для сканирования: маскирование, обрезка, масштабирование, выравнивание, устранение черной окантовки и связь с системой документооборота
ПО для улучшения и обработки изображений (по дополнительному заказу)	Интегрированное управление цветом, ORTHOSCAN (коррекция изгибов сканируемой книги), улучшение контраста, вращение изображения, функция очистки, устранения искажений, обрезка и масштабирование, маскирование, черно-белое сканирование с динамическим порогом чувствительности и т.д.
Электропитание	230 В, 50/60 Гц, 1.1 А. Другие напряжения по дополнительному запросу.
Габариты и вес широкоформатного сканера	OS10000 с OT180: 2625x1600x1600 мм (В x Д x Ш); Вес (без стола) примерно 180 кг.
Дополнительные принадлежности	ПО для интеграции сканера в систему электронного документооборота, ПО для улучшения изображения, лазерный принтер и рабочая станция

Зойчель Омнискан 11000

Широкоформатный цветной книжный сканер для библиотек и архивов

Каждый год тысячи и тысячи ценнейших книг, карт и документов в библиотеках и архивах приходят в негодность, проходя через множество людских рук, разрушаются от воздействия неблагоприятных условий хранения и использования. С исчезновением этих работ, мы навсегда теряем уникальную информацию, содержащуюся в них.

Широкоформатный цветной сканер Zeutschel Omniscan 11000 специально разработан для библиотек и архивов. Он предназначен для сканирования книг, газет и документов большого формата (карт, чертежей и т.п.), в том числе ветхих и поврежденных. Широкоформатный сканер Zeutschel Omniscan 11000 позволяет значительно повысить сохранность документов в библиотеках и архивах, благодаря очень деликатному обращению с оригиналами. В системе освещения отсутствует ультрафиолетовая компонента излучения, которая может повредить оригинал. Широкоформатный сканер Zeutschel Omniscan 11000 позволяет сканировать документы формата до 1092x914 мм всего за несколько десятков секунд. Широкоформатный сканер Zeutschel Omniscan 11000 удачно сочетает эргономичный дизайн с высочайшими стандартами оцифровки уникальных и бесценных документов.

Преимущества широкоформатного сканера

Zeutschel Omniscan 11000

- Максимальное разрешение 800 dpi
- Две трилинейные цветные CCD-матрицы – 21360 пикселей
- Различные настройки разрешения

- Меньше 60 секунд на сканирования документа формата A0/E при 300 dpi
- Бесконтактная сканирующая система

Технические характеристики сканера Zeutschel Omniscan 11000

Описание	Высокопроизводительная широкоформатный планетарный сканер (сканирующая система) для книг, газет и документов большого формата (чертежей, карт, документов)
Размер оригиналов	1092x914 мм
Сканирующая головка	Два трилинейных цветных CCD-сенсора высокого разрешения, 21360 пикселей (RGB), 36 битный цвет
Скорость сканирования	DIN A0/E при 200 dpi – 40 с (A1/C – 21 с); DIN A0/E при 300 dpi – 55 с (A1/C – 29 с); DIN A0/E при 400 dpi – 134 с (A1/C – 75 с).
Интерфейс широкоформатного сканера	SCSI-3 UltraFast
Формат изображений	Все стандартные форматы изображений: TIFF 6.0, JPEG, многостраничный TIFF, PDF, и т.д.
Сервер - Рабочая станция	Рекомендуется: процессор Pentium, частота больше 1000 МГц, 1 Гб оперативной памяти. Сервер по дополнительному запросу.
Прикладное ПО (по запросу)	OS 11 для высокой производительности со всеми стандартными инструментами для сканирования: маскирование, обрезка, масштабирование, выравнивание, устранение черной окантовки и связь с системой документооборота
ПО для улучшения изображений (по запросу)	Улучшение контраста, коррекция цвета, коррекция изгибов сканируемой книги, автоматическая обрезка и выравнивание, и т.д.
Стол сканера	Широкий выбор столов, стол с верхней подсветкой AT-0, книжная колыбель OT 180, OT 180 H и OT 180 H A0, стол с подсветкой (возможно со стеклянной пластиной), стол для газет (смотрите отдельную брошюру по столам серии OT). Специальные столы по дополнительному запросу.
Электропитание	230 В, 50/60 Гц, 180 Вт. Другие напряжения по дополнительному запросу.
Габариты широкоформатного сканера	OT 11000 с OT 180 H A0: 2530x1300x1000 мм (Д x Ш x В)

Зойчель Омнискан 14000 A0

Широкоформатный цветной книжный сканер для библиотек и архивов

Широкоформатный цветной планетарный сканер формата A0 Zeutschel Omniscan 14000 A0 специально разработан для библиотек и архивов. Он предназначен для сканирования книг, газет и документов большого формата (карт, чертежей и т.п.), в том числе ветхих и поврежденных.
Широкоформатный сканер Omniscan 14000 A0 позволяет значительно повысить сохранность документов в библиотеках и архивах, благодаря очень деликатному обращению с оригиналами. В системе освещения отсутствует ультрафиолетовая компонента излучения, которая может повредить оригинал. Широкоформатный сканер Omniscan 14000 A0 позволяет сканировать документы формата до 870x1240 мм за несколько секунд. Широкоформатный сканер Omniscan 14000 A0 удачно сочетает эргономичный дизайн с высочайшими стандартами оцифровки уникальных и бесценных документов.

Преимущества широкоформатного сканера
Zeutschel Omniscan 14000 A0

- Высокое разрешение - 400ppi
- Очень низкое воздействие излучения на оригинал
- Высокая производительность, в том числе благодаря функции ограничения области сканирования
- Скорость сканирования настраивается под ваши потребности
- Точное воспроизведение цветов оригинала
- Освещение активируется только на время сканирования
- Отсутствует ультрафиолетовая составляющая излучения
- Отсутствует тепловое воздействие излучения на оператора и оригинал

- Отсутствуют блики при сканировании глянцевых документов
- Очень удобная работа с прижимным стеклом благодаря эргономичной книжной колыбели Zeutschel
- Возможность работы без прижимного стекла
- Простое и эффективное программное обеспечение

Технические характеристики широкоформатного сканера

Zeutschel Omniscan 14000 A0

Описание	Высокопроизводительный широкоформатный планетарный сканер (сканирующая система) для книг, газет и документов большого формата (чертежей, карт, документов)
Размер оригиналов	870x1240 мм (>DIN A0/E)
Стол сканера	Широкий выбор столов, стол с верхней подсветкой AT-0, книжная колыбель OT 180 H/A0, колыбель для ветхих книг OT 90, стол с подсветкой (возможно со стеклянной пластиной), стол для газет (смотрите отдельную брошюру по столам серии OT)
Сканирующая головка	Высокопроизводительная сканирующая головка: высокоточные сканирующие линзы без искажений, глубина фокуса 50 мм, 36-битный цвет
Максимальное разрешение сканирования	400 dpi (до 600 dpi по дополнительному запросу)
Скорость сканирования	16.8 секунд при 400 dpi
Интерфейс широкоформатного сканера	2xFirewire
Формат изображений	Все стандартные форматы изображений: несжатый TIFF, TIFF G4, JPEG, многостраничный TIFF, PDF, BMP, PCX
Прикладное ПО	OS 12 64бит , для высокой производительности со всеми стандартными инструментами для сканирования: маскирование, обрезка, масштабирование, выравнивание, устранение черной окантовки и связь с системой документооборота
ПО для улучшения и обработки изображений (по дополнительному заказу)	Интегрированное управление цветом, ORTHOSCAN (коррекция изгибов сканируемой книги), улучшение контраста, вращение изображения, функция очистки, устранения искажений, обрезка и масштабирование, маскирование, черно-белое сканирование с

	динамическим порогом чувствительности и т.д.
Электропитание	230 В, 50/60 Гц, 1.1 А. Другие напряжения по дополнительному запросу.
Габариты	OS14000 с OT180: 2616x1564x1532 мм (В x Д x Ш);.
Дополнительные принадлежности	ПО для интеграции сканера в систему электронного документооборота, ПО для улучшения изображения, лазерный принтер и рабочая станция

Зойчель Омнискан 10000 A1

Широкоформатный цветной книжный сканер для библиотек и архивов

Преимущества широкоформатного сканера

Zeutschel Omniscan 10000 A1

- Очень низкое воздействие излучения на оригинал
- Высокая производительность, в том числе благодаря функции ограничения области сканирования
- Скорость сканирования настраивается под ваши потребности
- Точное воспроизведение цветов оригинала
- Освещение активируется только на время сканирования
- Отсутствует ультрафиолетовая составляющая излучения
- Отсутствует тепловое воздействие излучения на оператора и оригинал
- Отсутствуют блики при сканировании глянцевых документов
- Очень удобная работа с прижимным стеклом благодаря эргономичной книжной колыбели Zeutschel

- Возможность работы без прижимного стекла
- Простое и эффективное программное обеспечение

Технические характеристики широкоформатного сканера Zeutschel Omniscan 10000 A1

Описание	Высокопроизводительная широкоформатный планетарный сканер (сканирующая система) для книг, газет и документов большого формата (чертежей, карт, документов)
Размер оригиналов	871x610 мм (>DIN A1/D)
Стол сканера	Широкий выбор столов, стол с верхней подсветкой, книжная колыбель OT 180 H, колыбель для ветхих книг OT 90, стол с подсветкой (возможно со стеклянной пластиной), стол для газет (смотрите отдельную брошюру по столам серии OT)
Сканирующая головка	Высокопроизводительная сканирующая головка: 3x10424x7300 пикселей, высокоточные сканирующие линзы без искажений, глубина резкости 50 мм, 36-битный цвет
Максимальное разрешение сканирования	300 dpi (до 600 dpi по дополнительному запросу)
Скорость сканирования	10 секунд при 300 dpi
Интерфейс широкоформатного сканера	SCSI-3 Ultra Wide
Формат изображений	Все стандартные форматы изображений: несжатый TIFF, TIFF G4, JPEG, многостраничный TIFF, PDF, BMP, PCX
Прикладное ПО	OS 11 для высокой производительности со всеми стандартными инструментами для сканирования: маскирование, обрезка, масштабирование, выравнивание, устранение черной окантовки и связь с системой документооборота
ПО для улучшения и обработки изображений (по дополнительному заказу)	Интегрированное управление цветом, ORTHOSCAN (коррекция изгибов сканируемой книги), улучшение контраста, вращение изображения, функция очистки, устранения искажений, обрезка и масштабирование, маскирование, черно-белое сканирование с динамическим порогом чувствительности и т.д.
Электропитание	230 В, 50/60 Гц, 1.1 А. Другие напряжения по дополнительному запросу.
Габариты и вес	OS10000 с OT180:

широкоформатного сканера	2240x1280x1410 мм (В х Д х Ш); Вес примерно 180 кг.
Дополнительные принадлежности	ПО для интеграции сканера в систему электронного документооборота, ПО для улучшения изображения, лазерный принтер и рабочая

Зойчель ОС 12000 А1

Простой, быстрый и эффективный книжный сканер для библиотек и архивов

Преимущества книжного сканера Zeutschel OS 12000 A1

- Высокая скорость сканирования
- Низкое воздействие излучения (освещение активируется только во время сканирования)
- Нет чрезмерно яркого освещения и отсутствует тепловая нагрузка на сканируемый оригинал
- Отсутствует ультрафиолетовое излучение
- Прекрасные результаты сканирования
- Отсутствуют блики при сканировании глянцевых документов
- Совершенное освещение
- Легкая установка книжного сканера
- Отличное соотношение цены и качества

Технические характеристики книжного сканера Zeutschel OS 12000 A1

Описание	Планетарный книжный сканер настольного типа

	для сканирования книг, газет и крупноформатных документов (чертежи, карты и т.п.)
Размер области сканирования	846x600 мм (>DINA2)
Книжная колыбель	Максимальная толщина книги 170 мм, дополнительно доступна книжная колыбель с прижимным стеклом (возможно сканирование с или без стекла)
Автофокус	до 50 мм
Режимы сканирования	сканирование в 36-бит цвете, 12-бит оттенках серого,1-бит для черно-белых изображений
Разрешение	100–600 ppi
Скорость сканирования	5 с/300 ppi A1 в цветном режиме
Форматы изображений	Поддерживает все стандартные форматы, например не сжатые TIFF, TIFF G4,JPEG, JP2, многостраничные TIFF, PDF, BMP, PCS
Программное обеспечение	OS11 для повышения производительности
Обработка изображений / дополнительное программное обеспечение (предоставляется по дополнительному заказу)	Интегрированное управление цветом, совершенная система улучшения контрастности книг (коррекция изгибов сканируемой книги), вращение изображения, функция очистки, устранения искажений, обрезка и масштабирование, маскирование, черно-белое сканирование с динамическим порогом чувствительности и т.д.
Дополнительное оборудование	Персональный компьютер, монитор, рабочая станция
Интерфейс подключения к компьютеру	Firewire 1394, карта PCI и кабель входят в комплект поставки
Электропитание	230 В, 50/60 Гц, 1.1 А, другие диапазоны напряжений по запросу
Габариты книжного сканера	1130x1050x1500 мм (ширина x длина x высота)

ЗМІСТ