ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо збереження інформації, .

У публікації «Оценка эффективности систем защиты информации» розповідається, що різноманіття варіантів побудови інформаційних систем породжує необхідність створення різних систем захисту, та вимогають враховувати індивідуальні особливості кожної з них. Запропонована модель системи захисту інформації у вигляді тривимірної матриці.

У публікації «Правила безопасности для пользователей» запропоновано включити в Правила для користувачів, що розробляються в організації (фірмі), наступні розділи: рекомендації по закупівлі устаткування і програмного забезпечення, політика секретності, політика доступу, політика облікових записів, політика аутентифікації, політика порядку роботи, політика управління. Приведено перелік питань який необхідно відобразити в правилах, запропоновано чітко прописати відповідальність користувачів за певні дії, які піддають небезпеці інтереси організації (фірми).

У публікації «Защита информации в вашем компьютере» розповідається що найбільш потужними на сьогоднішній день вважаються засоби апаратного (фізичною) захисту інформації в комплексі з програмними засобами. Приведені їх описи.

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

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Источник: http://www.warning.dp.ua/comp9.htm
к.т.н. Домарев Валерий Валентинович domarev@protinfo.kiev.ua

Системный подход

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 системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.

Сегодня специалисты из самых разных областей знаний, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности. Это обусловлено тем, что в ближайшие лет сто нам придется жить в обществе (среде) информационных технологий, куда перекочуют все социальные проблемы человечества, в том числе и вопросы безопасности…

Каждый из указанных специалистов по-своему решает задачу обеспечения информационной безопасности и применяет свои способы и методы для достижения заданных целей. Самое интересное, что при этом каждый из них в своем конкретном случае находит свои совершенно правильные решения. Однако, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата - система безопасности в общем и целом работает не эффективно.

Если собрать всех специалистов вместе, то при наличии у каждого из них огромного опыта и знаний, создать СИСТЕМУ информационной безопасности зачастую так и не удается. Разговаривая об одних и тех же вещах, специалисты зачастую не понимают друг друга поскольку у каждого из них свой подход, своя модель представления системы защиты информации. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами защиты…

Постановка задачи.

Одиннадцать отдельно взятых футболистов (даже очень хороших) не составляют команду до тех пор, пока на основе заданных целей не будет отработано взаимодействие каждого с каждым. Аналогично СЗИ лишь тогда

станет СИСТЕМОЙ, когда будут установлены логические связи между всеми ее составляющими.

Как же организовать такое взаимодействие? В футболе команды проводят регулярные тренировки, определяя роль, место и задачи каждого игрока. Качество или эффективность команд оценивается по игре в матчах, результаты которых заносятся в турнирную таблицу. Таким образом, после проведения всех встреч команд (каждой с каждой), можно сделать вывод об уровне состояния мастерства как команды в целом, так и отдельных ее игроков. Побеждает тот, у кого наиболее четко организовано взаимодействие…

Выражаясь терминами современного бизнеса, для решения вопросов взаимодействия нужно перейти от "чисто" технического на "конкретно" логический уровень представления процессов создания и функционирования СИСТЕМ защиты информации. Хотелось бы, чтобы все специалисты, считающие себя профессионалами в информационных технологиях, поднялись чуть выше "багов" и "кряков" и уже сейчас задумались над тем как их знания и опыт будут логически увязаны со знаниями и опытом других специалистов.

В "строгой научной постановке" задача автора состоит в предоставлении пользователям вспомогательного инструмента "елки" - (модели СЗИ), а задача читателя (пользователя) - украсить эту "елку" новогодними игрушками - (своими знаниями и решениями). Даже если "игрушек" пока еще нет, наличие "елки" поможет выбрать и приобрести нужные "украшения".

Конечный результат работы (степень красоты елки) зависит от ваших желаний, способностей и возможностей. У кого-то получится хорошо, у кого-то - не совсем… Но это естественный процесс развития, приобретения знаний и опыта.

Кстати, оценить красоту елки (эффективность системы защиты) весьма проблематично, поскольку у каждого из нас свои требования и вкусы, о которых, как известно, не спорят, особенно с руководством.

Таким образом, многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время, большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Как сказал классик юмора: "…многообразие ваших вопросов порождает многообразие наших ответов…"

Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно что бы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые вкусы (требования) гурманов информационной безопасности?

Модель представления системы информационной безопасности.

Практическая задача обеспечения информационной безопасности состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС. Что понимается под моделью СЗИ? Насколько реально создать такую модель? В упрощенном виде модель СЗИ представлена на Рис.1.

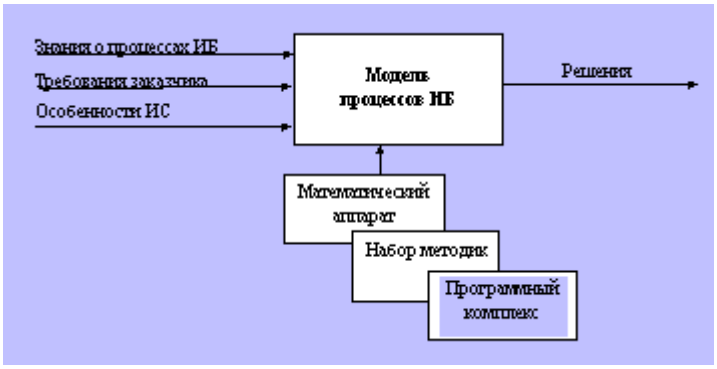


Рис.1. Модель СЗИ

Основной задачей модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Специфическими особенностями решения задачи создания систем защиты являются:

· неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;

· многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) СЗИ;

· наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ;

· невозможность применения классических методов оптимизации.

Требования к модели

Такая модель должна удовлетворять следующим требованиям (Рис. 2.):

Использоваться в качестве:

· Руководства по созданию СЗИ

· Методики формирования показателей и требований к СЗИ

· Инструмента (методика) оценки СЗИ

· Модели СЗИ для проведения исследований (матрица состояния)

Обладать свойствами:

· Универсальность

· Комплексность

· Простота использования
· Наглядность
· Практическая направленность
· Быть самообучаемой (возможность наращивания знаний)·
· Функционировать в условиях высокой неопределенности исходной информации

Позволять:
· Установить взаимосвязь между показателями (требованиями)
· Задавать различные уровни защиты
· Получать количественные оценки
· Контролировать состояние СЗИ
· Применять различные методики оценок
· Оперативно реагировать на изменения условий функционирования
· Объединить усилия различных специалистов единым замыслом

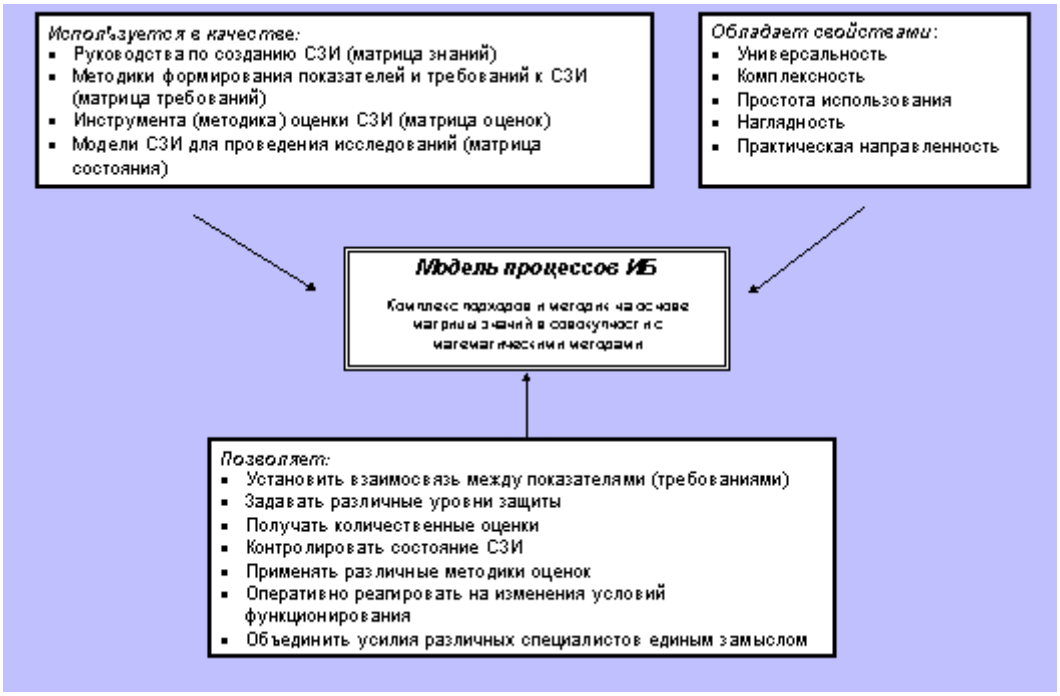


Рис. 2. Требования к модели СЗИ

Описание подхода к формированию модели ИБ

Как составить такое представление об информационной безопасности, что бы охватить все аспекты проблемы? Человек получает наиболее полное представление об интересующем его явлении, когда ему удается рассмотреть это нечто неизвестное со всех сторон, в трехмерном измерении.

Воспользуемся этим принципом.

Рассмотрим три "координаты измерений" - три группы составляющих модели СЗИ.

1. Из чего состоит (ОСНОВЫ)
2. Для чего предназначена (НАПРАВЛЕНИЯ)

3. Как работает (ЭТАПЫ)

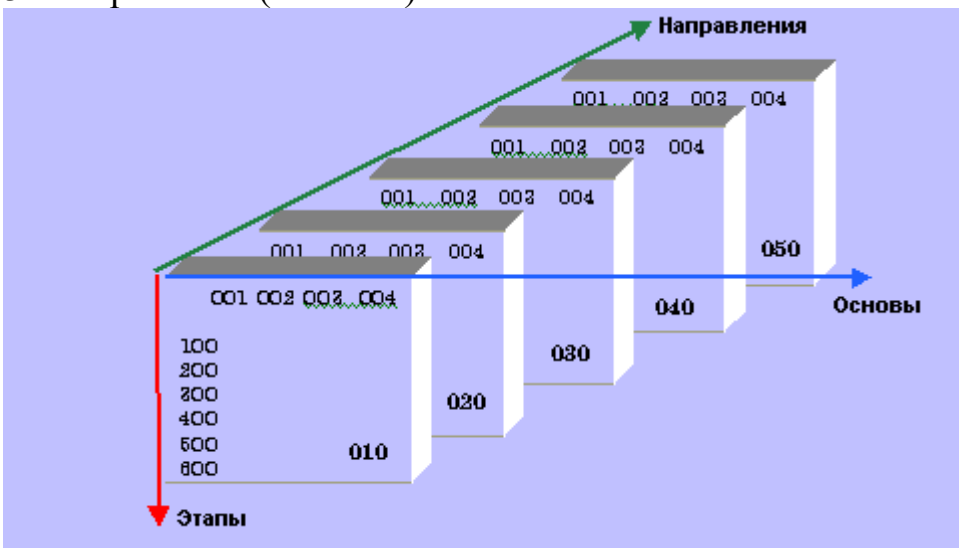


Рис. 3. Три "координаты измерений" - три группы составляющих модели СЗИ

ОСНОВАМИ или составными частями практически любой сложной 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 и методы (политика информационной безопасности);

· Программно-технические способы и средства.

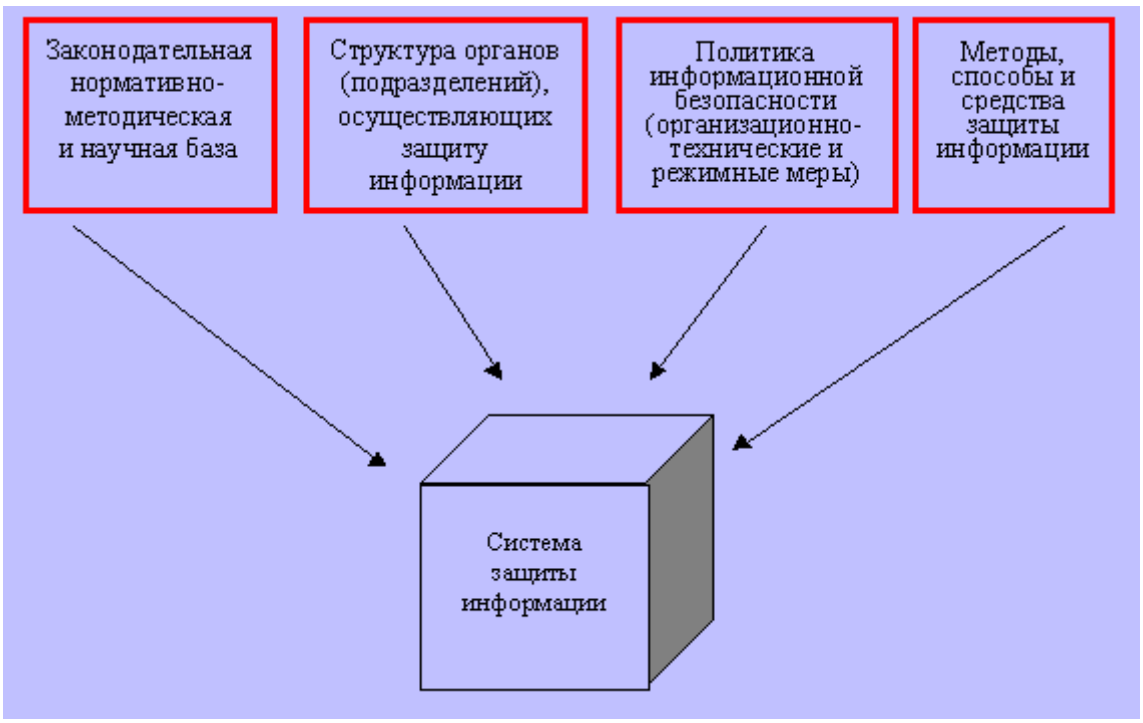


Рис. 4. Координата ОСНОВЫ

НАПРАВЛЕНИЯ формируются исходя из конкретных особенностей ИС как объекта защиты. В общем случае, учитывая типовую структуру ИС и исторически сложившиеся виды работ по защите информации, предлагается рассмотреть следующие направления:

· Защита объектов информационных систем;
· Защита процессов, процедур и программ обработки информации;
· Защита каналов связи;
· Подавление побочных электромагнитных излучений;
· Управление системой защиты.

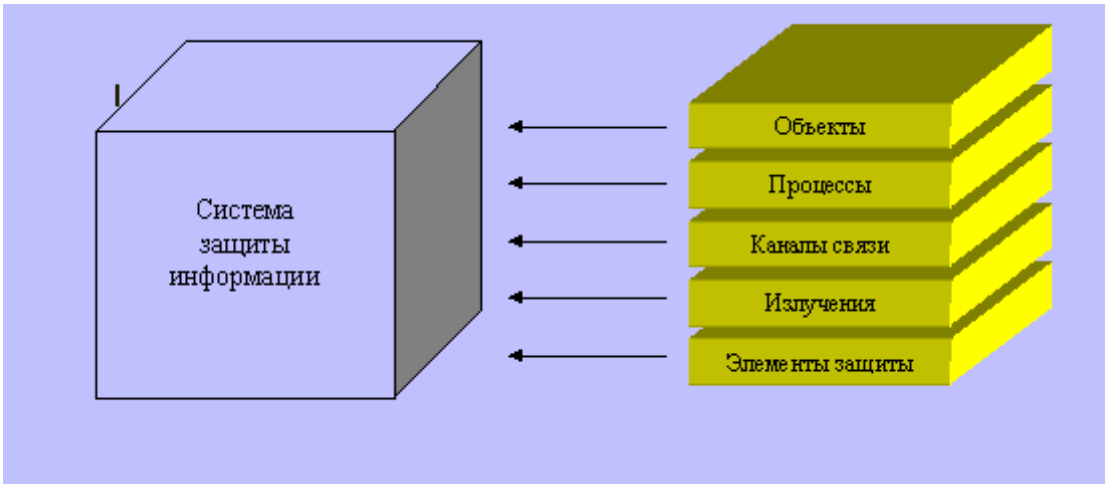


Рис. 5. Координата НАПРАВЛЕНИЯ

Но, поскольку каждое из этих НАПРАВЛЕНИЙ базируется на перечисленных выше ОСНОВАХ, то элементы ОСНОВ и НАПРАВЛЕНИЙ, рассматриваются неразрывно друг с другом. Например, одну из ОСНОВ под названием "Законодательная база…" необходимо рассматривать по всем НАПРАВЛЕНИЯМ, а именно:

Законодательная база защиты объектов;

Законодательная база защиты процессов, процедур и программ;

Законодательная база защиты каналов связи;

Законодательная база подавления побочных электромагнитных излучений;

Законодательная база по управлению и контролю самой системы защиты.

Аналогично следует рассматривать остальные грани ОСНОВ (структуру, меры, средства) по всем НАПРАВЛЕНИЯМ.

Как видите, для формирования самого общего представления о конкретной системе защиты необходимо ответить минимально на 20 (4*5=20) самых простых вопросов. Но и это еще не все. Далее необходимо рассмотреть ЭТАПЫ (последовательность шагов) создания СЗИ, которые необходимо реализовать в равной степени для каждого в отдельности НАПРАВЛЕНИЯ с учетом указанных выше ОСНОВ.

Проведенный анализ существующих методик (последовательностей) работ по созданию СЗИ позволяет выделить следующие ЭТАПЫ:

· Определение информационных и технических ресурсов, а также объектов ИС(!) подлежащих защите;

· Выявление полного множество 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.

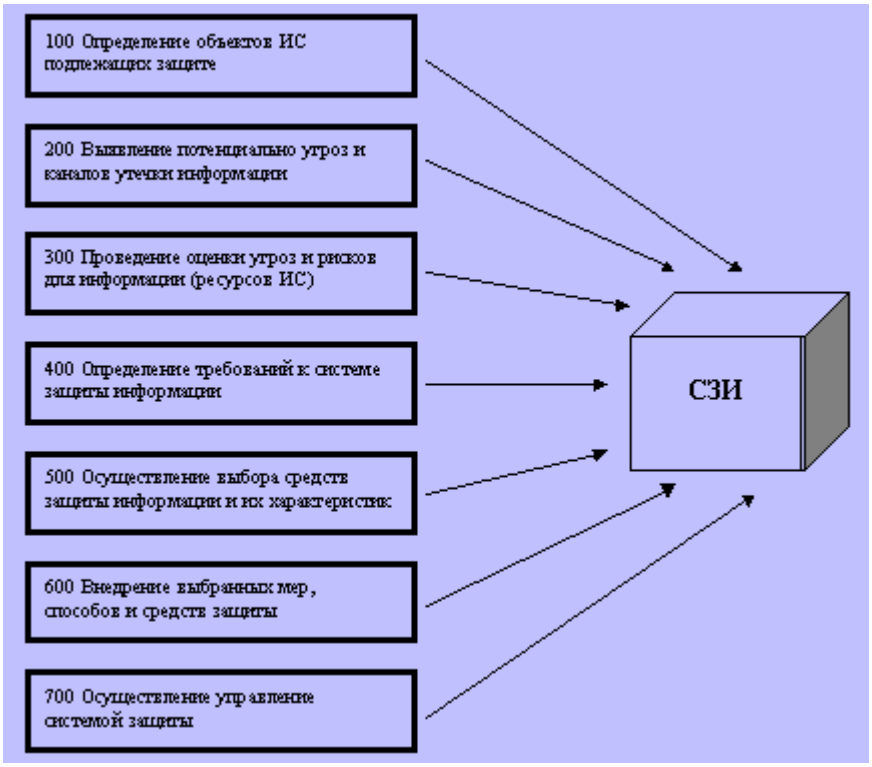


Рис. 6. Этапы создания систем защиты информации.

Поскольку ЭТАПОВ семь, и по каждому надо осветить 20 уже известных вам вопросов то в общей сложности для формирования представления о конкретной системе защиты необходимо ответить на 140 простых вопросов. Совершенно очевидно что по каждому вопросу (элементу) возникнет несколько десятков уточнений.

В общем случае количество элементов матрицы 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"

В нашем случае общее количество элементов "матрицы" равно 140

K=4*5*7=140.

поскольку Oi=4, Hj=5, Mk=7

Все это можно представить в виде своеобразного кубика Рубика, на гранях которого образовалась мозаика взаимосвязанных составляющих элементов системы защиты.

А теперь для простоты понимания попробуем преобразовать трехмерную фигуру в двухмерную. Для этого развернем трехмерный куб на плоскости (на листе бумаги) и получим трехмерную матрицу в виде двухмерной таблицы, которая поможет логически объединить составляющие блоков "ОСНОВЫ", "НАПРАВЛЕНИЯ" и "ЭТАПЫ" по принципу каждый с каждым.

Напомним, что матрица в виде двухмерной таблицы появляется не сама по себе, а формируется в каждом конкретном случае, исходя из конкретных задач по созданию конкретной СЗИ для конкретной ИС.

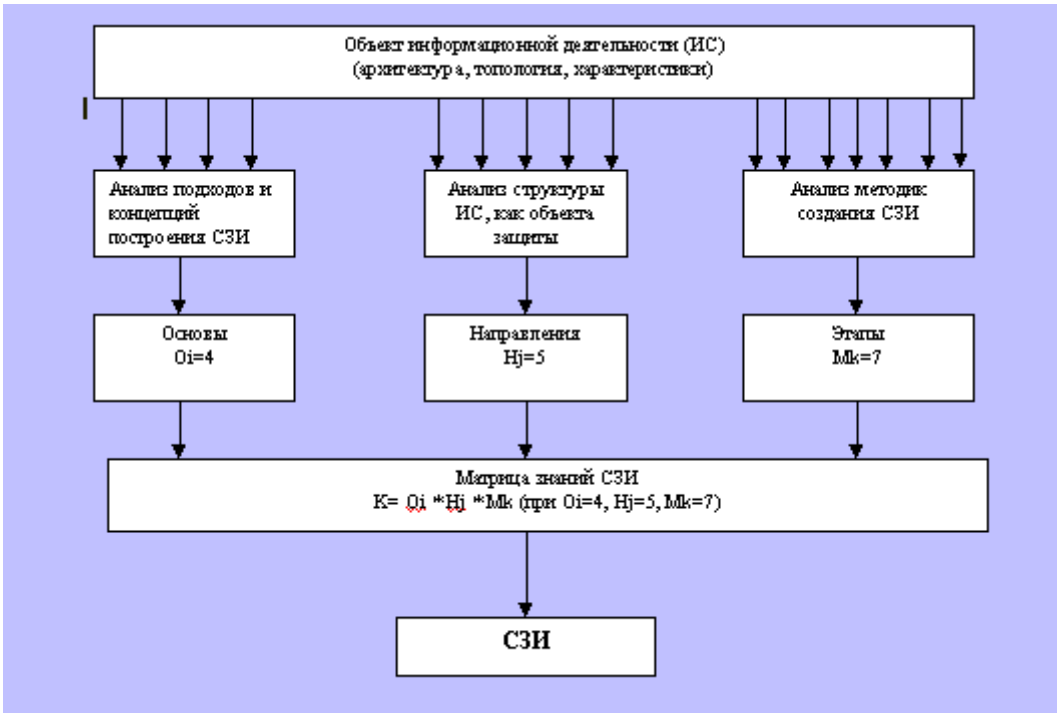


Рис. 7 – Матрица СЗИ для объекта информационной деятельности

Представление элементов матрицы

Элементы матрицы имеют соответствующую нумерацию. Следует обратить внимание на обозначения каждого из элементов матрицы, где:

первое знакоместо (X00) соответствует номерам составляющих блока "ЭТАПЫ",

второе знакоместо (0X0) соответствует номерам составляющих блока "НАПРАВЛЕНИЯ",

третье знакоместо (00X) соответствует номерам составляющих блока "ОСНОВЫ".

Элемент матрицы 321 формируется с учетом следующих составляющих:

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

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

001 - Нормативная база (составляющая № 1 блока "ОСНОВЫ")

Приведем пример содержания информации для элементов матрицы № 321, 322, 323, 324, которые объединяют следующие составляющие: № 3 (300 проведение оценки уязвимости и рисков) блока "ЭТАПЫ", № 2 (020 защита процессов и программ) блока "НАПРАВЛЕНИЯ" № 1, 2, 3, 4 (001 нормативная база, 002 структура органов, 003 мероприятия, 004 используемые средства) блока "ОСНОВЫ".

Вот что получилось:

Элемент № 321 содержит информацию о том 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 ИС?

Элемент № 322 содержит информацию о том имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для процессов и программ ИС?

Элемент № 323 содержит информацию о том определены ли режимные меры, обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

Элемент № 324 содержит информацию о том применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведения оценки уязвимости и рисков в процессах и программах ИС?

Это содержание только четырех вопросов из ста сорока, но ответы на них уже позволяют сформировать некое представление о состоянии дел по защите информации в конкретной ИС.

В общем случае рассматриваются все 140 вопросов (по числу элементов матрицы). Полное содержание 140 элементов матрицы можно посмотреть здесь. Описание этих вопросов позволяют составить полное представление о СЗИ и оценить достигнутый уровень защиты.

Сложно? Да! Однако именно такой подход дает возможность держать правильное направление в процессе создания сложных систем защиты. "…

Верной дорогой идете, товарищи…". А поскольку при этом постоянно учитываются взаимные логические связи между многочисленными элементами СЗИ, то есть шанс построить именно СИСТЕМУ, а не набор решений. Напомним, что матрица не сществует сама по себе, а формируется исходя из описания конкретной ИС и конкретных задач по защите информации в этой системе, см. рисунок 8:

Свойства матрицы

Предложенная модель представления СЗИ в виде трехмерной матрицы позволяет не только жестко отслеживать взаимные связи между элементами защиты, но может выступать в роли руководства по созданию СЗИ. Если вы, приступая к созданию системы защиты, не знаете с чего начать, попробуйте ответить на предлагаемые общие вопросы, начиная с любого из них. И когда вы пройдетесь по всем, то поймете что уже есть, а чего не хватает для достижения поставленной цели.

Наглядно указанные свойства матрицы приведены на Рис.8.

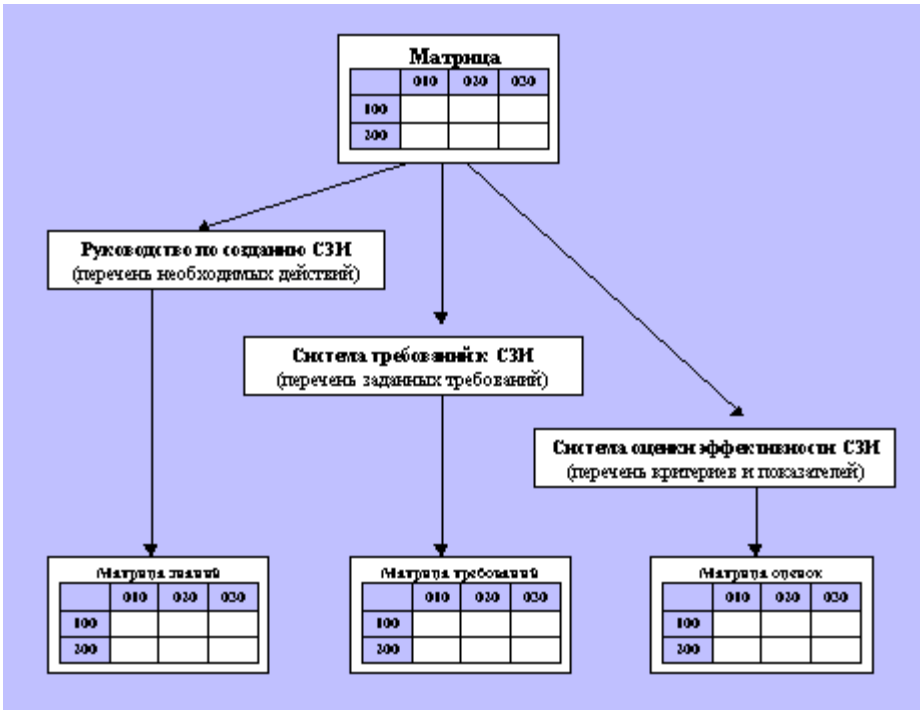


Рисунок 8. Свойства матрицы информационной безопасности

Если желаете поставить задачу на создание СЗИ, то заполнив 140 элементов матрицы соответствующими требованиями, получим достаточно полное техническое задание. Причем сформулировать эти требования можно на основе любых стандартов - международных, европейских, американских, российских, украинских.

Ну а как оценить эффективность создаваемой или уже функционирующей СЗИ?

Снова поможет подход на основе трехмерной матрицы. Только теперь по 140 показателям (элементам матрицы) надо выставить соответствующие оценки. Существует много методов оценок, выбирайте любой понятный и

прозрачный для вас. Наиболее популярный на сегодняшний день метод "Три П" - пол, палец, потолок.

Программа оценки эффективности систем защиты информации "Оценка СЗИ"

Программа "Оценка СЗИ" иллюстрирует работу модели СЗИ представленной в виде трехмерной матрицы, описание которой приведено выше, она разработана с целью демонстрации преимуществ системного подхода к созданию и оценке эффективности систем защиты информации. С помощью указанной программы осуществляется расчет условных показателей эффективности СЗИ, а также графическое представление состояния достигнутого уровня безопасности по отношению к заданному.

Программа "Оценка СЗИ" реализована на языке программирования Delphi и предназначена для оценки эффективности мероприятий, проводимых при создании и функционировании систем защиты информации.

Предложенная модель СЗИ в виде трехмерной матрицы позволяет не только жестко отслеживать взаимные связи между элементами защиты, но может выступать в роли руководства по созданию СЗИ. Если вы, приступая к созданию системы защиты, не знаете с чего начать, попробуйте ответить на предлагаемые в матрице вопросы, начиная с любого из них. И когда вы пройдетесь по всем вопросам, то поймете что уже сделано, а чего не хватает для достижения поставленной цели.

Если желаете поставить задачу на создание СЗИ, то заполнив 140 элементов (вопросов) матрицы соответствующими требованиями, получим достаточно полное техническое задание. Причем сформулировать эти требования можно на основе любых стандартов - международных, европейских, американских., российских, украинских…

Ну а как оценить эффективность создаваемой или уже функционирующей СЗИ?

Снова поможет подход на основе трехмерной матрицы. Только теперь по 140 показателям (элементам матрицы) надо выставить соответствующие оценки. Существует много методов оценок, выбирайте любой понятный и прозрачный для вас. Наиболее популярный на сегодняшний день метод "Три П" - пол, палец, потолок.

Интерфейсы программы с некоторыми комментариями представлены на рисунках 9, 10, 11, 12.

При внимательном рассмотрении можно узнать уже знакомую нам "матрицу знаний СЗИ" в несколько другом представлении.

На Рис. 9. показан интерфейс ввода данных. Заказчик определяет необходимые требования к системе защиты и устанавливает заданный уровень безопасности в соответствующие элементы матрицы. Экесперты в процессе проведения оценки качества созданной системы защиты определяют реализован ли заданный уровень безопасности и свои оценки выставляют в тех же элементах матрицы, только в режиме "достигнутый"

Рис. 9. Интерфейс ввода данных

На рис. 10 можно посмотреть графическеое представление количественных и качественных оценок по каждому из элементов матрицы. Здесь наглядно показано как сравнивается заданный уровень безопасности с достигнутым.

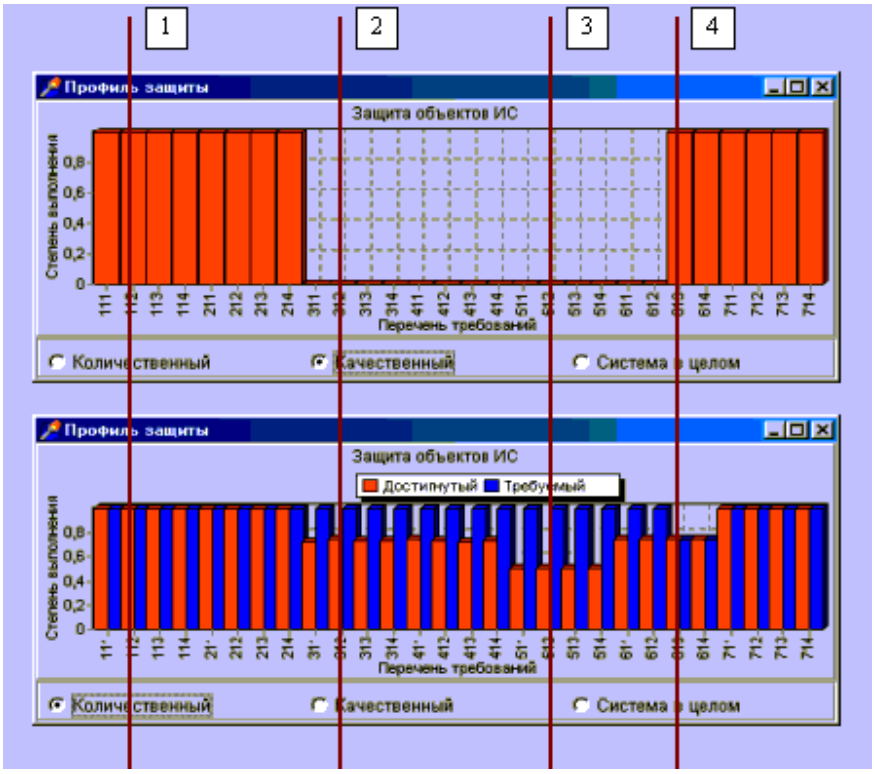


Рис. 10. Сравнение заданного и достигнутого уровеней безопасности.

Далее с помощью интерфейса на рис 11. имеется возможность получить представление о ситеме защиты в целом. Ее эффектиность наглядно отражена графически, а также расчитана в виде обобщенных показателей уровня безопаности (количественного и качественного)

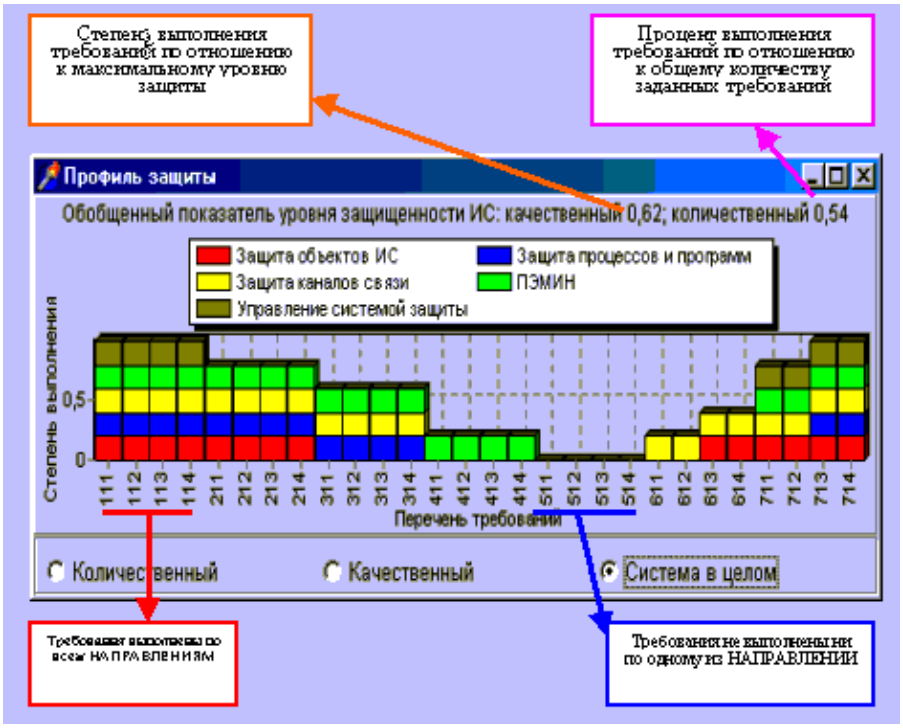


Рис. 11. Графичекое представление оценки эффективности СЗИ.

Не стоит забывать, что требования к СЗИ имеют разную степень важности, которую необходимо учитывать при расчетах, используя соответствующие коэффициенты важности. Интерфес для ввода коэффициентов важности представлен на рис. 12.

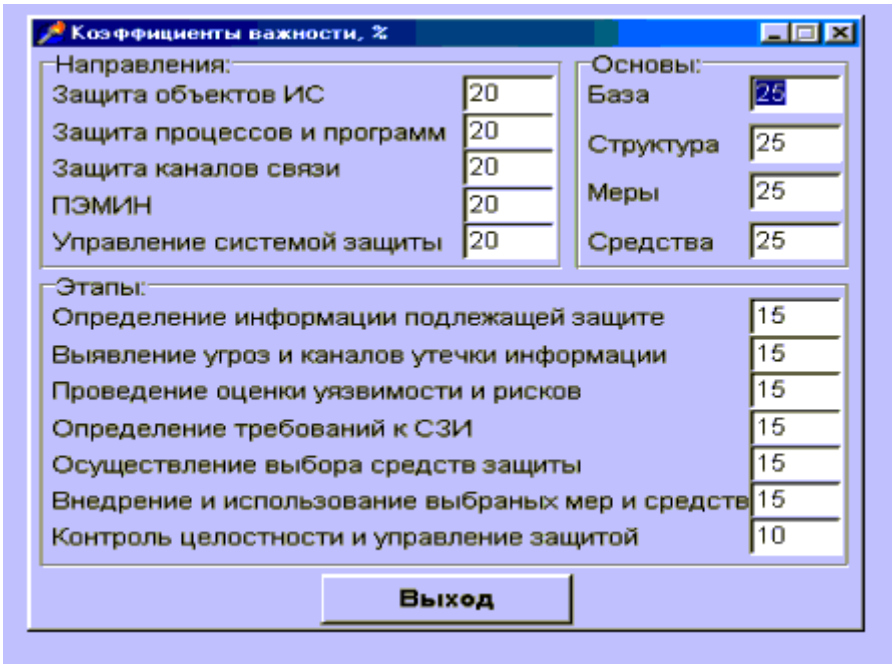


Рис. 12. Интерфес для ввода коэффициентов важности.

Вместо заключения (Read me)…

Хочется напомнить золотое правило: если после долгих попыток ничего не получается, ознакомьтесь, наконец, с инструкцией для пользователя! Прежде чем приступить к использованию программы "Оценка СЗИ", желательно разобраться с особенностями похода к рассмотрению вопросов информационной безопасности, предложенного автором.

Здесь можно скачать EXE-файл указанной программы оценки эффективности систем защиты информации. (680 793 байт)

Программа предназначена для свободного использования...

ПРАВИЛА БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Источник: http://www.warning.dp.ua/comp14.htm

В 1997 году одна из подгрупп IETF выпустила справочник Site Security Handbook (RFC-2196). В нем содержатся рекомендации системным администраторам по разнообразным вопросам защиты сети, правилам использования и методике работы. По существу это важная часть политики безопасности. Такая политика всегда содержит перечень запретов и ограничений. Политика всегда должна быть явно прописанной. Желательно, чтобы были прописаны отдельно правила для работы с серверами (файлами), электронной почтой, системой Instant Messaging, P2P (если использование этой техники вообще разрешено) и т.д. В большинстве стран руководитель организации несет ответственность за действия сотрудников, если они наносят другой организации или частным лицам существенный ущерб. Важно, чтобы все сотрудники понимали причины вводимых ограничений, а для этого необходимо регулярно проводить обучение персонала. Этот документ предлагает включить в правила следующие разделы:

- ***Рекомендации по закупке оборудования и программного обеспечения***. Участие системных администраторов в выборе оборудования и программного обеспечения может оказать большую пользу, так как часто они знают о его недостатках и ограничениях то, чего не афишируют продавцы и производители.
- ***Политика секретности***. Устанавливает степень контроля над почтой и действиями пользователей, а также политику размещения пользовательских файлов.
- ***Политика доступа***. Определяет, кто может иметь доступ в систему, что можно делать в рамках этих прав доступа, какое программное обеспечение можно установить и пр. Данный документ должен включать те

же меры предосторожности относительно авторизации доступа и степени контроля, что и политика секретности.

- ***Политика учетных записей***. Содержит описание прав и обязанностей пользователей и системных администраторов.
- ***Политика аутентификации***. Устанавливает правила использования паролей и порядка лишения доступа.
- ***Политика доступа***. Определяет, в какое время система должна быть доступна, содержит расписание обслуживающих мероприятий, перечень действий при появлении проблем, а также инструкции по документированию проблем и оповещению о них администраторов и ориентировочное время их устранения.
- ***Политика управления***. Устанавливает правила общения с внешним миром и порядок доступа для приглашенных из других организаций специалистов.

Помимо названных рубрик может присутствовать политика использования e-mail, IM и других сервисов. Вообще говоря, из соображений безопасности может быть введена фильтрация содержимого любых входящих и исходящих сообщений (порнография, сетевые игры и пр.). Допустимо введение ограничений на используемые языки. Целесообразно четко прописать ответственность пользователей за определенные действия, которые подвергают опасности интересы организации (фирмы) или отдельных лиц. Можно напомнить пользователям правила поведения воспитанных людей в сети. (Netiquete)

Правила для пользователей

В правилах для пользователей необходимо регламентировать следующие вопросы:

- Использование учетных записей совместно с друзьями и родственниками.
- Выполнение программ дешифрования паролей для расшифровки локального файла **passwd,** например, с помощью программы **crack.**
- Выполнение программ дешифрования паролей для расшифровки файлов **passwd** других систем.
- Нарушение нормального процесса обслуживания.
- Проникновение в чужие учетные записи.
- Неправильное использование электронной почты.
- Просмотр файлов других пользователей (есть ли возможность чтения? записи? одобряется ли?)
- Публикации в UseNet (запрещены? с оговорками? разрешены?)
- Импорт программ из Интернет (запрещен? разрешен? разрешен с оговорками?)
- Использование системных ресурсов (принтеров, дисков, модемов, процессора).
- Копирование лицензионного программного обеспечения.
- Выдача разрешений на копирование лицензионного программного обеспечения другим лицам.

- Копирование защищенных авторскими правами материалов (музыки, фильмов и пр.).
- Всевозможная незаконная деятельность: мошенничество, клевета и др.
- Вовлечение в деятельность, которая является запрещенной (например, порнография)

Примером соглашения для доступа к компьютерам может служить документ такого рода для факультета информатики университета Мельбурна. Смотри также http://www.admin.com.

Я, нижеподписавшийся, настоящим объявляю, что буду придерживаться приведенных ниже правил:

- Я буду использовать возможности компьютеров и сети факультета исключительно для учебных целей, относящихся к моему обучению информатике.
- Я знаю, что факультет предоставляет регистрационное имя для его использования исключительно получателем. По этой причине я не буду способствовать использованию моей учетной записи и файлов другими лицами и сообщать свой пароль кому бы то ни было.
- Я не буду осуществлять доступ или попытку доступа ни к одному компьютеру, регистрационной записи, сети или файлу без соответствующего и явного разрешения. Такой доступ является незаконным и противоречит университетским правилам. Если мне станет известно, что такой доступ имел место, я немедленно проинформирую об этом руководство факультета.
- Я знаю, что некоторые программы и данные, находящиеся в файловой системе, могут быть защищены законом об авторских правах и другими законами или лицензионными соглашениями. Я не буду нарушать накладываемые ими ограничения.
- Я не буду использовать университетские ресурсы для получения, разработки, запуска и распространения нелицензионного программного обеспечения.
- Я обязуюсь сохранять конфиденциальность любых полученных мною от университета сведений о программном обеспечении (включая методы и принципы его использования), лицензионном для использования на ЭВМ университета, и тем самым обезопасить университет от претензий любого рода, связанных с разглашением этой информации.
- Я обязуюсь проявлять предельную честность и порядочность во всех вопросах, связанных с использованием компьютерных и сетевых возможностей университета, которые могут повредить репутации факультета или университета.
- Я понимаю, что действия, противоречащие изложенным выше принципам, повлекут за собой жесткие взыскания, включая отказ в изучении темы или предмета, временный запрет или лишение доступа к университетским вычислительным средствам, временное или полное исключение из университета, штраф и/или другие действия,

предусмотренные Crimes Computer Act (этот закон действует в Австралии, но аналогичные законы имеются во многих других странах) 1988 года

Обратите внимание на неоднозначные слова о честности, порядочности и необходимости беречь репутацию университета. Подобные требования общего характера помогают охватить вопросы, которые трудно описать строгими детерминированными правилами. И хотя юридическая сила таких требований невелика, все же полезно их включить во внутренние правила компании или учреждения. Заверенная расписка пользователя о согласии следовать перечисленным правилам является юридическим документом и может использоваться в суде. Обязательно нужно проинформировать всех пользователей, что сам факт использования учетной записи, равносилен согласию соблюдать установленные правила. Должно быть известно, где можно ознакомится с правилами. Следует иметь в виду, что не имеющие юридической силы и противоречивые правила - хуже, чем их отсутствие.

Здесь нет ни слова об использовании программ сканирования, рассылки сообщений содержащих “троянских коней” или вирусы, попыток взлома защиты серверов и пр. Это все преступления, которые обычно регламентируются уголовным кодексом. И следует учитывать, что оправдания типа, я решил просто посмотреть, как работает такая программа из любопытства и т.д., не могут служить оправданием. Полагаю, никто не воспримет серьезно оправдание вроде: “Я хотел лишь проверить, работает ли этот гранатомет, у меня и в мыслях не было разносить вдребезги эту бензоколонку…”

Не нужно думать, что права системных администраторов не ограничиваются ничем. Если системный администратор злоупотребляет своими полномочиями, им следует подобрать другую работу. Если специфика работы требует наличия нескольких администраторов, пароль root помещается в конверт, а конверт в сейф. Администраторы же пользуются программой **sudo**. Если в какой-то момент времени кому-то потребуется пароль root, конверт извлекается из сейфа, и после завершения операции пароль заменяется.

Рекомендуется помещать в файл /etc/motd (сообщение дня) предупреждение о действующих у вас правилах. Предупреждение должно содержать перечень мер, которые будут предприняты, при несоблюдении правил (удаление учетной записи, размер штрафа или уголовная ответственность).

Работа в экстренных ситуациях

Следует решить заблаговременно вопрос о том, кто должен руководить работами в экстремальной ситуации, определить субординацию. Имена и телефоны должностных лиц также как базовые IP-адреса следует хранить вне системы. Возможно, там (вне сети) следует держать и конфигурационную базу данных. Обычно руководитель ВЦ для этих работ не пригоден. Должно быть известно, где хранятся последние backup-копии жизненно важных частей ОС (помимо файла **/etc/dumpdates**). На случай взлома WEB-сервера известной компании, нужно тщательно продумать тактику контакта со

средствами массовой информации, клиентами. Это все настолько важно, что стоит подумать о необходимости специальных учений. Часто в таких ситуациях поток запросов серверу может резко возрасти (многие любопытные пытаются проверить слух об аварии, а слухи в сети распространяются как снежная лавина). Если ваш сервер не в полной мере восстановлен и излишняя загрузка для него губительна, позаботьтесь о переадресации избыточной части запросов на другой сервер, который будет уведомлять: “Извините, узел перегружен и в данный момент мы не можем обработать ваш запрос”. Рекомендуется использовать программу **tripwire**, чтобы согласовать действия системных администраторов, особенно если разные группы администраторов отвечают за разные аспекты работы одной ЭВМ. Например, “заплаты” СУБД Oracle и ОС могут конфликтовать друг с другом. В результате одна группа, поставившая “заплату” может и не подозревать, что текущая проблема является следствием действий другой группы. Программа **tripwire** идентифицирует, что и когда изменялось, и помогает доказать администраторам, что именно их действия явились причиной неполадок.

Приложение. Пример политики в отношении электронной почты

1. E-mail должна использоваться только для в служебных целях. Любое использование почты в частных целях может производиться только в случае, если это разрешено действующими правилами. Пользователям запрещается применять какие-то свои почтовые программы (например, hotmail и пр.).
2. Сотрудникам может быть разрешено общаться со своими супругами, детьми и другими родственниками, но при этом время использования e-mail должно ограничиваться обеденным перерывом. Запрещается посредством почты осуществлять сбор благотворительных средств или искать другую работу.
3. Почта подготовленная к отправке на компьютере компании или пришедшая извне может просматриваться или фильтроваться. Сотрудники не могут рассчитывать на конфиденциальность своих почтовых обменов. В связи с этим запрещается использовать шифрование (например, PGP).
4. Компания может мониторировать и архивировать весь почтовый обмен без уведомления об этом сотрудников. Компания имеет право раскрывать содержимое частного обмена, если это затрагивает интересы фирмы, предьявлять эти данные в суде, если это потребуется.
5. Запрещается рассылка оскорбительных сообщений или информации, носящий дискриминационный характер, или призывающей к насилию.
6. Администрации предприятия запрещается:

- Рассылать, копировать, печатать тексты или грфические объекты, которые порочат кого-либо на основе рассовой, религиозной, сексуальной ориентации, возраста, происхождения или национальной принадлежности.
- Рассылать или распространять сообщения унижающие или оскорбляющие кого-либо.

- Распространять слухи или намеки о сотрудниках клиентах или партнерах.
- Рассылать тексты или изображения сексуального характера.

7. Несмотря на ограничения конфиденциальности администрация должна исключить утечку персональных данных.
8. Сотрудники не должны пересылать по почте любую конфиденциальную информацию, касающуюся фирмы или ее сотрудников.
9. Электронной почтой не следует пользоваться при взаимодействии с юристами (запросы рекомендаций или консультаций).

Смотри также www.stbernard.com.

ЗАЩИТА ИНФОРМАЦИИ В ВАШЕМ КОМПЬЮТЕРЕ

Источник: http://www.warning.dp.ua/hackPC01.htm

Если программа глючит, значит, она неверная.
Неверные программы надо стереть.
Безглючны только верные программы.
Если верная программа выдает, что 2x2=5, значит, глючат все программы, дающие другие результаты.
(Ислам /сунниты/ глазами программиста)

Наиболее мощными на сегодняшний день считаются средства аппаратной (физической) защиты информации в комплексе с программными средствами.

Примечание. *Заранее оговорю маленькую деталь – все программные средства ЗИ этой и следующей частей рассматриваются на примере IMB-совместимой архитектуры и ОС Microsoft Windows 2000 Server.*

Аппаратные средства защиты

1. Запрет доступа к КС посторонних лиц

Одно из самых простых и относительно надежных средств ЗИ. Заключается в оборудовании помещений с КС сигнализацией, постоянной охраной, закрытии серверных стоек на замок при покидании помещения ответственными лицами, а также постоянном контроле над теми, кто имеет доступ к защищаемой КС и т.п.

2. Электронно-механические ключи для запуска ПК

В этот метод входят как различные электронные ключи, блокирующие загрузку ПК, так и обычные механические блокираторы клавиатуры, кнопки включения питания и т.п. В случае с электронными ключами системный блок

ПК стараются расположить, например, в стальном шкафу, называемым серверной стойкой.

Программные средства защиты

3. Установка паролей на начальную загрузку ПК

- ***Теория***. BIOS – это комплекс аппаратно-программных средств, предназначенный для тестирования аппаратной составляющей компьютера и загрузки ОС. Т.е. по сути это программа, расположенная в постоянной памяти на материнской плате; точнее в полу-постоянной, т.к. обычно BIOS поддерживает обновление – т.н. "прошивку". Это первая программа, запускаемая при включении питания ПК. Используется для инициализации и тестирования аппаратного обеспечения (POST-процедура), а также загрузки и запуска ОС. Все начальные настройки оборудования (они же настройки BIOS) хранятся в энергозависимой памяти CMOS. Для защиты ПК – BIOS поддерживает установку двух типов паролей:

- User Password – пароль на возможность начальной загрузки ПК, запрашивается после тестирования аппаратного обеспечения и собственно перед загрузкой любой ОС.

- Supervisor Password – пароль полного доступа к BIOS, он же пароль администратора BIOS, включает в себя возможность изменения настроек BIOS и возможность начальной загрузки ПК.

- ***Цель***. Запрет загрузки операционной системы без пароля, тем самым обеспечивается относительная защита данных даже на FAT-разделах, а также дополнительная аутентификация пользователей не зависимо от средств самой ОС, установленной на ПК.

- ***Методика***.

1) Для входа в режим редактирования настроек BIOS нажимайте клавишу <Delete> в процессе начальной загрузки ПК до появления меню настройки BIOS.

2) Для задания любого из паролей выберите требуемый вам пункт меню (**Set User Password**[a] и/или **Set Supervisor Password**). Установите нужный вам пароль(и).

3) Сохраните внесенные изменения, нажав клавишу <F10>, или выберите пункт меню **Save and Exit Setup** [**Exit Saving Changes**]. После этого ПК перезагрузится.

4. Запрет загрузки ПК с дискеты

- ***Теория***. Как известно ОС можно загрузить не только с жесткого диска, а, например, с дискеты, получив тем самым доступ к данным на диске (причем даже на NTFS-разделах – *см. подробнее Глава 9.3 PAGEREF _Ref49331336 \p \h на стр. 293*). Данный метод следует использовать в комплексе с предыдущим; т.о. если злоумышленник будет иметь пароль начальной загрузки (пусть даже пароль пользователя), а загрузка с других устройств, отличных от жесткого диска, будет разрешена – он элементарно

сможет загрузиться с одного из них (напр. с дискеты) и получить доступ к данным на диске.

- ***Цель***. Запрет загрузки ПК с устройств отличных от жесткого диска, тем самым обеспечение относительной безопасности данных в ПК.

- ***Методика***.

1) Войдите в режим настройки BIOS *(см. Пункт 3.1 выше)*.

2) Затем в секции **Advanced BIOS Features** [**Boot**] пункты **Legasy Floppy**, **CD-ROM** и т.п. имена устройств нужно убрать с первой позиции в **Boot Sequence**[§] чтобы попытка загрузки с них не была первой (**First Boot Device** – должен быть обязательно ваш жесткий диск).

3) Сохраните внесенные изменения BIOS *(см. Пункт 3.3 выше)*.

5. Шифрование защищаемой информации

- Теория. *См. "Криптографическая ЗИ" PAGEREF _Ref49343587 \p \h на стр. 277.*

- ***Цель***. Защита данных при хранении/передаче/транспортировке.

- ***Методика***. Существуют программные комплексы, предоставляющие возможность шифрования данных "на лету". Вы можете выделять свободное место на разделах жесткого диска для шифруемых данных. При этом создается зашифрованный файл, который представляется в системе в виде отдельного виртуального раздела (тома). Зашифрованный том ведет себя как обычный раздел системы, но отличается от обычных разделов тем, что перед монтированием используется аутентификация паролем или устройствами аппаратной аутентификации (требуется поддержка АО и ПО). Шифрование данных при работе с томом прозрачно для пользователя и происходит "на лету". При выборе программы обратите внимание на спецификации криптоалгоритмов, поддерживаемые ею (*см. "Криптосистемы и принцип шифрования" PAGEREF _Ref49343354 \p \h на стр. 278)*.

Наиболее удачные программы этого класса:

- BestCrypt 7
- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.
- Технические характеристики:

- Комплексное ПО, содержит в себе 4 разнофункциональных модуля;

- (1) Модуль шифрования данных – менеджер виртуальных дисков;

- (2) Модуль скрытых контейнеров – возможность создания скрытого контейнера внутри обычного контейнера (стенографический метод);

- (3) Модуль невосстановимого удаления данных – удаление файлов или папок, своп-файла;

- (4) Модуль шифрования своп-файла;

- Автоматическое закрытие открытых контейнеров по клавише-сочетанию и таймеру;

- Модуль защиты созданных контейнеров от случайного удаления в проводнике ОС;

- Полная интеграция с оболочкой (англ.: Shell) Windows;

- Создание ссылок на контейнеры (напр., расположенные в сети), а также групп ссылок;

- Алгоритмы шифрования: Rijndael (AES), Blowfish, Twofish, ГОСТ 28147-89.

- Стандарты уничтожения данных:

- Американский 7-ми проходный метод DoD 5220.28-STD (с возможностью ручного указания количества проходов).

- Преимущества:

- Удобный в использовании и понятный интерфейс. Выбор автора!

- Недостатки:

- Невозможность динамически изменять размер созданных разделов;

- "Непрозрачное" для пользователя создание виртуальных дисков и их форматирование.

- Официальный сайт: http://www.jetico.com/.

- **SafeHouse Drive Encryption 2.10**

- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.

- Технические характеристики:

- Размеры создаваемых разделов до 2048 Гб (для ОС Win NT/2000/XP) и до 4 Гб (для Win 9x);

- До 10 одновременно подключенных разделов для Win 9x/Me и более – для Win NT/2000/XP;

- Динамическое изменение размера созданных разделов;

- Поддержка X.9 устройств аппаратной аутентификации;

- Полная интеграция с оболочкой Windows;

- Размеры ключей до 448 бит;

- Административное получение доступа к зашифрованным дискам, используя открытые/закрытые ключи на базе алгоритма Диффи-Хеллмана.

- Алгоритмы шифрования: Rijndael (AES), Blowfish, Twofish, DES, 3-DES.

- Преимущества:

- Довольно высокая скорость шифрования данных;

- Удобный визард-подобный интерфейс. Выбор автора!

- Официальный сайт: http://www.pcdynamics.com/safehouse/.

- **Steganos Safe 5**

- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP (Home & Professional).

- Технические характеристики:

- Комплексное ПО, содержит в себе 3 разнофункциональных модуля;

- (1) Модуль шифрования данных – менеджер виртуальных дисков, поддерживающий до 4 дисков максимальным размером 1,2 Гб;

- (2) Модуль переноса данных – позволяет создать портативный зашифрованный контейнер с данными, который поддерживает саморасшифровывание;

- (3) Модуль невосстановимого удаления данных – удаление файлов или папок с файлами;

- Алгоритмы шифрования: Rijndael (AES), 128-бит.
- Стандарты уничтожения данных:

- Стандартная однопроходная процедура перезаписи;
- Американский многопроходный метод DoD 5220.22-M/NISPOM 8-306.

- Преимущества:

- Абсолютно "прозрачное" для пользователя создание вирт. дисков и их форматирование.
- Очень удобный в использовании интерфейс в стиле Windows XP.

- Недостатки:

- Маленькое количество контейнеров, поддерживаемых одновременно;
- Невозможность динамически изменять размер созданных разделов.

- Официальный сайт: http://www.steganos.com/.

6. Стеганографирование защищаемой информации

- ***Теория***. *См. "Стеганография или еще один шаг на пути ЗИ" PAGEREF _Ref49594061 \p \h на стр. 282.*
- ***Цель***. Сокрытие и шифрование секретных данных от посторонних глаз.
- ***Методика***. Программное обеспечение:

- **SecurEngine 4.0**
- Технические характеристики:

- Комплексное ПО, содержит в себе 5 разнофункциональных модулей;
- (1) Модуль сокрытия данных – позволяет скрывать данные в файлах, поддерживаемые форматы BMP, JPEG, TXT, WAV;
- (2) Модуль шифрования данных;
- (3) Модуль невосстановимого удаления данных;
- (4) Модуль создания саморасшифровывающихся архивов;
- (5) Модуль безопасного хранения паролей – позволяет хранить логины, пароли и УРЛ вэб-страниц;
- После операции возможно невосстановимое удаление оригинала, либо обычное удаление.

- Алгоритмы шифрования: 3-WAY, Blowfish, CAST256, GOST, MARS256, VERNAME.
- Стандарты уничтожения данных:

- Национальный американский стандарт уничтожения DoD 5220.22-M;
- Стандартная 1-3-5-7-9-ти проходная процедура перезаписи.

- Официальный сайт: http://securengine.isecurelabs.com/.
- **MP3Stego**
- Технические характеристики:

- Скрытие данных в музыкальных файлах. Вначале данные сжимаются, шифруются, и только потом скрываются в WAV-файле, который затем конвертируется в MP3 файл;

- Стандарты обработки данных.

- Сжатие данных – алгоритм ZLIB;

- Шифрование – криптоалгоритм 3-DES.

- Официальный сайт: http://www.petitcolas.net/fabien/steganography/mp3stego/index.html/.

7. Невосстановимое удаление данных

- ***Теория***. *См. "Невосстановимое удаление данных" PAGEREF _Ref52634043 \p \h на стр. 283*.

- ***Цель***. Навсегда стереть секретные данные с носителей информации.

- ***Методика***. Программное обеспечение:

- **Acronis Drive Cleanser 6.0**

- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP, Linux (все дистрибутивы), FreeBSD, Solaris, SCO UNIX, UNIXWARE, OS/2, BeOS, QNX, B-TRON.

- Технические характеристики:

- Гарантированное удаление всех данных и разделов на жестком диске. Внимание +программа полностью удаляет все данные с выбранного раздела(ов) или раздел(ы) целиком;

- Возможность наряду с очисткой отформатировать диск или раздел диска, или удалить оный;

- Возможность увидеть результаты выполнения сценария уничтожения информации раздела и/или жесткого диска с помощью встроенной программы DiskViewer.

- Стандарты уничтожения данных.

- 5 национальных стандартов уничтожения данных:

- Американские – DoD 5220.22-M, NAVSO P-5239-26 (RLL), NAVSO P-5239-26 (MFM);

- Германский – VSITR;

- Российский – GOST P50739-95.

- Два значительно более мощных предопределенных алгоритма, предложенных наиболее авторитетными экспертами по информационной безопасности:ости:

- Алгоритм Питера Гутмана;

- Алгоритм Брюса Шнайера.

- Простой, но быстрый алгоритм для использования в менее важных ситуациях – Быстрый.

- Преимущества: Очень удобный в использовании интерфейс в стиле Windows XP.

- Официальный сайт: http://www.acronis.ru/products/drivecleanser/.

- **BCWipe 3.0**
- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.
- Технические характеристики:
- Является частью программного комплекса BestCrypt Data Encryption System.
- Гарантированное удаление файлов и/или папок;
- Гарантированное удаление всех данных с выбранного раздела(ов);
- Очистка содержимого своп-файла.
- Преимущества: Полная интеграция с оболочкой Windows, понятный интерфейс.
- Официальный сайт: http://www.jetico.com/.

- **File Shredder 2000 v 3.4**
- Поддерживаемые ОС: Win 9x/Me/2000/XP.
- Стандарты уничтожения данных:
- Стандартная 2-х проходная процедура очистки;
- 7-ми проходный метод удаления файлов, одобренный NSA.
- Недостатки: Жуткий интерфейс а-ля Windows 95, отсутствие деинсталлятора.
- Официальный сайт: http://www.gregorybraun.com.

8. Установка прав доступа к защищаемому ресурсу внутри системы

- ***Теория***. В ОС семейства Microsoft Windows NT и файловой системой NTFS каждый объект защищен от попыток несанкционированного доступа путем разделения прав доступа. У объекта есть владелец (по умолчанию тот, кто его создал), а также пользователи, которые имеют некоторые права доступа к нему (например, просмотр содержимого каталога, модификация оного и т.п.).

- Внимание! *Не забывайте, когда вы будете болеть или шеф вызовет вас к себе на ковер, добрый коллега Вася вполне может изменить или похитить вашу информацию, сидя за вашим же компьютером.*

- ***Цель***. Запрет (полный или частичный) другим пользователям системы доступа к данным.

- ***Методика***.

1) Выберите необходимую папку с данными. Определитесь в круге лиц и правах доступа, которые они будут иметь. Никогда **+** не назначайте пользователям права большие, чем им необходимо!

2) В проводнике кликните правой кнопкой мыши на защищаемом ресурсе и выберите из появившегося контекстного меню пункт **Свойства** (англ.: **Properties**). В открывшемся диалоге перейдите на вкладку **Безопасность** (англ.: **Security**).

3) В появившемся диалоге установите права доступа к защищаемому ресурсу: выберите пользователей или группу оных (кнопка **Добавить…**, англ.: **Add…**), а также укажите их полномочия – полный доступ, изменение,

чтение и запуск программ в папке, просмотр содержимого папки, чтение, запись.

4) Нажмите кнопку <OK> для вступления в силу проделанных изменений.

9. Установка прав доступа к защищаемому ресурсу по сети

- ***Теория***. К каждому объекту в ОС семейства Microsoft Windows NT и файловой системой NTFS можно открывать доступ по сети. Т.е. пользователи других ПК по сети могут спокойно работать с данными, находящимися на вашем ПК. Процесс открытия доступа пользователям сети называется "Расшариванием" от англ.: Share.

- ***Внимание!*** *Наиболее распространенный способ хищения информации, не нуждающийся в особых умениях – это кража из "расшаренной" папки. Так что, если надумаете расшарить свою личную папку, внимательно посмотрите список субъектов, имеющих к ней доступ. Это же касается системных администраторов! По умолчанию, их папки расшариваются системой с полным доступом для членов группы Администраторов. А так ли вам необходимо, чтобы ваш шеф (он то малый неплохой, но большой зануда и атеист) читал ваши любовные послания к Маше с 3-го подъезда или сокральные тексты древнего происхождения?*

- ***Цель***. Полный или частичный запрет другим пользователям системы доступа к данным по сети.

- ***Методика***.

1) Выберите необходимую папку с данными. Определитесь в круге лиц и правах доступа, которые они будут иметь. Никогда + не назначайте пользователям права большие, чем им необходимо! Не расшаривайте + папки в системных разделах жесткого диска, где расположена ваша(и) ОС.

2) В проводнике кликните правой кнопкой мыши на защищаемом ресурсе и выберите из появившегося контекстного меню пункт **Свойства** (англ.: **Properties**). В открывшемся диалоге перейдите на вкладку **Общий доступ** (англ.: **Sharing**).

3) В появившемся диалоге установите права доступа к защищаемому ресурсу: выберите пользователей или группу оных (кнопка **Добавить…**, англ.: **Add…**), а также укажите их полномочия – полный доступ, изменение, чтение и запуск программ в папке, просмотр содержимого папки, чтение, запись.

4) Нажмите кнопку <OK> для вступления в силу проделанных изменений.

10. Установка прав доступа к учетной записи (только для Администраторов)

- ***Теория***. Уважаемые господа Администраторы! К вам обращено сие послание. Если вы думаете, что имея учетную запись администратора – вы "пуп земли", то вы глубоко ошибаетесь. Многие забывают про небольшую деталь. Учетные записи также являются + защищаемыми объектами,

поэтому они также имеют свойства **Безопасности** (англ.: **Security**). Пусть вы закрыли доступ к своим личным данным внутри системы и доступ по сети, но остается эта небольшая лазейка для похитителя, также владеющего административными привилегиями. Начнем с того, что он может просто сменить ваш пароль, тем самым получив доступ к вашей информации. Но смена пароля – это нездоровая тенденция, умные люди делают по-другому: создается временная учетная запись администратора (около 1-2 мин.), затем в вашей учетной записи устанавливаются доверительные отношения к созданной записи, и воа-ля – врата открыты. Теперь похититель имеет законный доступ к вашей информации. Дальше дело воображения и времени, можно достучаться к ней по сети (так более надежно) или с вашего ПК (если папка не "расшарена"). После хищения нужной информации, временная учетная запись удаляется.

- ***Цель***. Запрет контроля вашей учетной записи другими администраторами системы.

- ***Методика***.

1) "Пуск Программы Администрирование Пользователи и Компьютеры Active Directory". Перейдите к элементу списка **Пользователи** (англ.: **Users**). И найдите свою учетную запись.

2) Кликните правой кнопкой мыши на выбранной записи и выберите из появившегося контекстного меню пункт **Свойства** (англ.: **Properties**). В открывшемся диалоге перейдите на вкладку **Безопасность** (англ.: **Security**).

3) В появившемся диалоге установите полные права доступа только для вас, всех остальных пользователей необходимо удалить, в том числе и **+ Систему** (англ.: **System**). Обычно *главные* системные администраторы идентифицируют свою учетную запись как **Системную**, тем самым получая полный контроль над системой и ее составляющими.

4) Нажмите кнопку <ОК> для вступления в силу проделанных изменений.

11. По WWW без следов

- ***Теория***. *См. "Пару слов об Интернете" PAGEREF _Ref54109338 \p \h на стр. 283*.

- ***Цель***. Сокрытие посещенных веб-страниц, а также личных данных при посещении Интернета.

- ***Методика***.

Удаление следов производится следующим образом. Откройте "Пуск - Панель управления - Свойства обозревателя". В появившемся диалоге нажмите кнопки <Удалить "Cookie"> и <Удалить файлы>. В результате будут удалены все файлы из папки временных файлов Интернета, а также файлы Cookie. Отключить сохранение временных файлов можно нажав на кнопку <Параметры…> и установив флаг "Никогда", а также задать размер занимаемого места на диске равным 0.

Также уничтожьте все компрометирующие посещения Интернета из журнала посещенных страниц. Откройте Internet Explorer. Меню "Вид-

Панели обозревателя-Журнал". Затем в появившемся окне выберите и удалите нужные записи из журнала. Они разбиты по дням и страничкам.

Вышеприведенная методика используется восновном для "чужих" компьютеров. У себя же дома или в офисе можно использовать специализированные программы для очистки следов деятельности в Интернете. Из них наиболее популярные и эффективные:

- **Acronis Privacy Expert 2003**
- Поддерживаемые ОС: Win 9x/Me/NT/2000/XP.
- Технические характеристики:

- Определяемый пользователем уровень безопасности;
- Утилита очистки по расписанию;
- Полная зачистка свидетельств работы в системе и Интернете с отдельно указываемыми пользователем областями данных для очистки;
- Комплексное ПО, содержит в себе 2 разнофункциональных модуля:
- (1) Очистка Интернет-компонентов:
- **Уникально** – поддержка браузеров Internet Explorer®, Netscape® 4, 6, 7, и Mozilla®;
- Очистка Интернет кэша;
- Очистка "ключиков" (cookies);
- Очистка Истории и последних посещенных страниц в Интернете;
- Удаление ActiveX компонентов;
- Очистка списка автозаполнения Internet Explorer®;
- Очистка списка предыдущего поиска в Internet Explorer®.
- (2) Очистка компонентов системы:
- **Уникально** – надежное затирание свободного места на диске и уничтожение удаленных файлов, во избежание их восстановления;
- **Уникально** – полное уничтожение задаваемых файлов и папок;
- Постоянная очистка файла подкачки;
- Надежная очистка Корзины;
- Очистка папок для временных файлов;
- Очистка списка найденных файлов;
- Очистка списка найденных компьютеров;
- Очистка списка запускаемых команд Windows;
- Очистка списка последних использованных документов;
- Очистка истории Общего диалога (последние посещенные места, история открытия/сохранения);
- Очистка резервных копий реестра;
- Удаление всех свидетельств поиска файлов на подключенных дисках и сетевых компьютерах;
- Стандарты уничтожения данных.

5 национальных стандартов уничтожения данных:

- Американские – DoD 5220.22-M, NAVSO P-5239-26 (RLL), NAVSO P-5239-26 (MFM);
- Германский – VSITR;

- Российский – GOST P50739-95.

- Два значительно более мощных предопределенных алгоритма, предложенных наиболее авторитетными экспертами по информационной безопасности:

- Алгоритм Питера Гутмана;

- Алгоритм Брюса Шнайера.

- Простой, но быстрый алгоритм для использования в менее важных ситуациях – Быстрый.

- Преимущества: Очень удобный в использовании интерфейс в стиле Windows XP. Выбор автора.

- Официальный сайт: http://www.acronis.ru/products/privacyexpert/.

- **Steganos Internet Trace Destructor 6.5**

- Поддерживаемые ОС: Win 9x/Me/2000/XP.

- Технические характеристики:

- Очистка Интернет кэша;

- Очистка "ключиков" (cookies) с возможностью выбора;

- Очистка Истории и последних посещенных страниц в Интернете;

- Очистка "следов" от программ Media-Player, WinZIP, WordPad, Google Toolbar, T-Online и AOL;

- Очистка содержимого своп-файла и временных файлов.

- Невосстановимое удаление выбранных "следов";

- Является частью пакета Steganos Internet Anonym 5 *(см. ниже)*.

- Официальный сайт: http://www.steganos.com/en/itd/.

- **Steganos Internet Anonym 5**

- Поддерживаемые ОС: Win 9x/Me/2000/XP.

- Технические характеристики:

- Комлексное ПО для прозрачного посещения Интернета;

- Поддержка браузеров Internet Explorer®, Netscape® и Mozilla®;

- Блокировка всплывающих окон (реклама и т.п.);

- Блокировка опасного содержимого: останов ActiveX и JavaScript;

- Анонимность в видео-конференциях;

- Очистка "следов" от программ AOL, Office 2000 и XP, Media Player, WinZIP, Google Toolbar и др.

- Возможность динамической смены личной информации для внешней сети (Интернета);

- Невосстановимое удаление выбранных "следов";

- Включает в себе Steganos Internet Trace Destructor 6 *(см. выше)*.

- Официальный сайт: http://www.steganos.com/en/siapro/.

12. Советы системным администраторам

- Запретите пользователям + оставлять на рабочих местах (в ч.с. корпусах мобильных компьютеров) памятки, содержащие идентификаторы и пароли доступа в корпоративную сеть и т.п.

- Никогда + не пишите пароль пользователя в графе Комментарий (англ.: Comment) и т.п. графах.

- Установите блокировку учетной записи пользователей после 5 неудачных попыток входа на 30 мин. Этим вы защититесь от метода перебора паролей. Однако это не касается + учетной записи Администратора, в ч.с. если он имеет право доступа через сеть – это открывает лазейку для взломщика.

- Переименуйте учетную запись Администратор.

- Отключите учетную запись Гость.

- Запретите Администратору вход через сеть.

- Запретите передачу SMB пакетов через TCP/IP, порты: 137,138,139.

- Установите аудит событий, при этом периодически просматривайте журналы событий.

Примечание:

[a] Здесь и далее в квадратных скобках будут указаны возможные названия пунктов меню. В разных версиях BIOS и у разных производителей эти названия могут варьироваться.

[§] Boot Sequence (англ.) – последовательность начальной загрузки системы, определяет последовательность опроса накопителей для загрузки с них ОС. Эти устройства обозначаются либо буквами для физических жестких дисков и обычных дисководов, либо названием устройства, например "CDROM". Поддерживаются устройства LS-120, Iomega ZIP, ATAPI CD-ROM, IDE- и SCSI-диски. В некоторых версиях BIOS опция "Boot Sequence" трансформировалась в несколько самостоятельных опций: "First Boot Device", "Second Boot Device", "Third Boot Device", "Boot Other Device".

[¨] Своп файл, файл подкачки (англ.: Swap file) – файл поддержки виртуальной памяти, в нем хранятся все данные, которые не помещаются в оперативную память.

ШИРОКОФОРМАТНЫЕ СКАНЕРЫ

Источник: http://www.storage-systems.ru/scanners/largescanners/. Продолжение, начало в Информационных бюлетенях № 3 и № 4 за 2016 год.

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

ЦС Архив А СЛ300

Широкоформатный сканер

Технические характеристики широкоформатного сканера Cruse CS Archive A SL300

Модель	Максимальный формат оригинала (см)	Максимальное оптическое разрешение для оригинала макс. формата (dpi)
CS 90A SL300	50 x 70	150 / 300 / 600
CS 110A SL300	A1 59,4 x 84	150 / 300 / 600
CS 145A SL300	A0 84 x118,8	150 / 300 / 600

Синхрон Тэйбл Е 300

Широкоформатный сканер

Технические характеристики широкоформатного сканера

Cruse Synchron Table E 300

Модель	Максимальный формат оригинала (см)	Максимальное разрешение сенсора (пиксел)	Максимальное оптическое разрешение для оригинала макс. Формата (dpi)	Максимальный размер файла при сканировании 3 x 8 бит (МБайт)
CS 130ST E300	70 x 100	8 400 x 12 000	300	300
CS 145ST E300	84 x 120	10 000 x 14 500	300	430
CS 155ST E300	92 x 122	10 800 x 14 500	300	460
CS 185ST E300	100 x 150	12 000 x 18 000	300	650
CS 220ST E300	120 x 180	14 000 x 21 000	300	900

ЦС Синхрон Тэйбл СТ МС

Широкоформатный сканер

Технические характеристики широкоформатного сканера Cruse CS Synchron Table ST MS

Модель	Макси-мальный формат оригинала (см)	Макси-мальный формат оригинала (дюйм)	Сканирование оригинала максимального формата			Сканирование с разрешением 600 dpi	
			Разре-шение	Пик-сел	Раз-мер файла	Пиксел	Размер файла 3x8 бит
CS 155T620	92x 122	36 x 48	300	10800x 14400	445	10800x 28800	890
CS 185ST1100	100x15	40x60	300	12000x 18000	615	14000x 36000	1440
CS 220ST1100	120x180	48x72	300	14000x 21600	865	14000x 43200	1730
CS 285ST1100	150x225	60x90	230	14000x 20700	830	14000x 54000	2160
CS 295ST1100	150x250	60x96	230	14000x 22700	880	14000x 59100	2500
CS 310ST1100	180x250	72x96	190	14000x 18700	730	14000x 59100	2500
CS 360ST1100	200x300	80x120	175	14000x 21000	840	14000x 72000	2880

ЦС Синхрон Тэйбл СТ Репро Декор

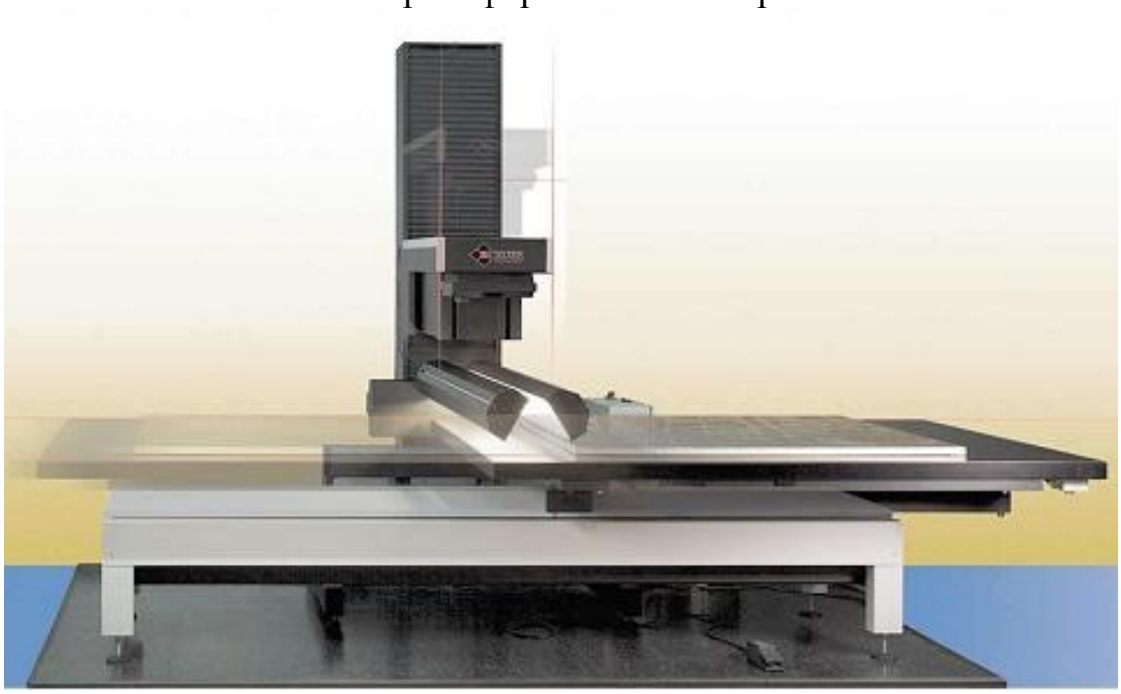
Широкоформатный сканер

Технические характеристики широкоформатного сканера Cruse CS Synchron Table ST Repro Decor

Модель	Максимальный формат оригинала (см)	Максимальное разрешение сенсора (пиксел)	Максимальное оптическое разрешение для оригинала макс. формата (dpi)	Максимальный размер файла при сканирова-нии 3 х 8 бит (МБайт)
CS 130ST775	70 x 100	12 00 x 22 200	420	775
CS 155ST775	92 x 122	12 000 x 22 000	330	775
CS 155ST1100	92 x 122	14 000 x 26 640	380	1100
CS 185ST775	100 x 150	12 000 x 22 200	300	775
CS 185ST1100	100 x 150	14 000 x 26 640	350	1100
CS 220ST775	120 x 180	12 000 x 22 200	250	775
CS 220ST1100	120 x 180	14 000 x 26 640	300	1100
CS 285ST1100	150 x 225	14 000 x 26 640	240	1100

ЦС Синхрон Тэйбл СТ ВР

Широкоформатный сканер



Технические характеристики широкоформатного сканера Cruse CS Synchron Table ST VR

Модель	Максимальный формат оригинала (см)	Максимальное разрешение сенсора (пиксел)	Максимальное оптическое разрешение для оригинала макс. формата (dpi)	Максимальный размер файла при сканировании 3 x 8 бит (МБайт)
CS 130ST530	70 x 100	10 000 x 14 300	360	420
CS 145ST530	92 x 122	10 000 x 143000	300	420
CS 155ST620	92 x 122	10 800 x 14 400	300	450
CS 185ST775	100 x 150	12 000 x 18 000	300	650
CS 185ST1100	100 x 150	14 000 x 21 000	350	900
CS 220ST775	120 x 180	12 000 x 18 000	250	650
CS 220ST1100	120 x 180	14 000 x 21 000	300	900
CS285ST1100	150 x 225	14 000 x 21 000	240	900
CS 295ST1100	150 x 250	14 000 x 23 500	240	990

ЦС Экономи Сканер Е ФЛ300

Широкоформатный сканер

Технические характеристики широкоформатного сканера Cruse CS ECONOMY Scanner E FL300

Модель	Максимальный формат оригинала (см)	Максимальное оптическое разрешение для оригинала макс. формата (dpi)
CS 110E FL300	A1, 59,4 x 84	150 / 300 / 600
CS 145E FL300	A0, 84 x 118,8	150 / 300 / 600

SupraScan Quartz A1

Широкоформатный сканер

Широкоформатный сканер SupraScan Quartz A1 для оригиналов формата до A1 позволяет оцифровывать широкоформатные книги, фолианты, манускрипты, карты и произведения искусства, а также полупрозрачные оригиналы.

Технические характеристики сканера SupraScan Quartz A1

Способ сканирования	Планетарный, бесконтактный, реверсный (двунаправленный), с синхронной подсветкой
Максимальный размер области сканирования, мм	630 x 840
Тип фотосенсора	CCD, RGB 3x10200 pix
Максимальное оптическое разрешение, без интерполяции, dpi	A1 – 400, A2 – 600, A3 – 800, A4 - 1000
Тип осветителя	Синхронно перемещаемый с зоной сканирования, LED с переключаемыми режимами освещения поверхности
Режимы освещения	5 режимов: Максимальный, универсальный (вкл. глянцевые док-ты), бестеневой, 2 текстурных режима

Глубина цвета (внутр.)	42 бита на пиксель
Режимы сканирования	Монохромный, полутоновый, цветной
Обработка изображения	- автоматическая обрезка по формату - выравнивание текста - корректировка кривой изгиба переплета - балансировка по белому, цветокоррекция в реальном времени
Управление цветопередачей	Гамма-коррекция, ICC-профили
Скорость сканирования, сек, полноцветный режим	A1/400dpi - 7,9 сек A1/300dpi - 6 сек
Дополнительные функции и модули	- стол подсветки прозрачных оригиналов - книжная колыбель автоматизированная для оригиналов толщиной 50 см - цветовые мишени Color Checker 24 для калибровки - USB педаль управления - рабочая станция, мышь и клавиатуру и монитор - держатель для книг с разворотом
Электропитание В/Гц	220/50, 500ВА
Вес	310 кг

ЗМІСТ