Об авторе

Домарев Валерий Валентинович

Получив высшее образование инженера по радиоэлектронике, длительное время занимался разработкой и эксплуатацией автоматизированных систем управления военного назначения.

В структуре Министерства Обороны Украины, а затем в Государственном комитете Украины по вопросам государственных секретов и технической защиты информации, занимался вопросами внедрения современных информационных технологий, а так же поиском путей обеспечения безопасности информации при создании и эксплуатации компьютерных систем.

В течение последних 10 лет работал над решением вопросов защиты информации в государственных информационно-управляющих системах различного уровня. Осуществлял руководство рядом научно-исследовательских работ по проблемам обеспечения безопасности современных информационных технологий.

Связаться с автором можно по E-mail:
domarev@protinfo.kiev.ua
или через http://www.security.ukrnet.net

Посвящение

Посвящается моей семье, родным и близким, которые помогали мне морально и материально во время работы над очередной книгой. Надеюсь, что их терпение окупится, а потраченное мною время не пропадет зря.

Благодарности

Выражаю свою искреннюю признательность и благодарность за помощь в создании книги:

Ананскому Евгению Викторовичу, заместителю директора ООО "КВИРИН", за консультации и огромную помощь в написании раздела книги, посвященного вопросам технического шпионажа;

Барсуковскому Юрию Владимировичу, кандидату технических наук, президенту фирмы "Бартек", за поддержку в создании книги;

Бурдыкину Станиславу Владиславовичу, директору фирмы "Бумекс";

Витанову Красимиру Методиеву, президенту компании "Геос-Информ";

Герасимову Борису Михайловичу, доктору технических наук, профессору, заслуженному деятелю науки и техники Украины, за то, что он посвятил меня в таинство математических формул и зависимостей;

Горбенко Ивану Дмитриевичу, доктору технических наук, профессору, зав. кафедрой Харьковского Государственного университета радиоэлектроники;

Дворецкому Георгию Алексеевичу, сотруднику фирмы "Энран-телеком";

Качко Елене Григорьевне, профессору кафедры программного обеспечения ЭВМ Харьковского Государственного университета радиоэлектроники, специалисту в области системного программирования и разработки программных систем защиты информации.

Колобову Сергею Александровичу, начальнику отдела Департамента специальных телекоммуникационных систем и защиты информации СБ Украины;

Короленко Михаилу Петровичу, начальнику центра технической защиты информации ОАО "КП ВТИ";

Кузнецову Георгию Витальевичу, доктору технических наук, профессору, академику Украинской Академии информатики, за понимание и моральную поддержку;

Ланде Дмитрию Владимировичу, кандидату технических наук, зам. директора ООО "ElVisti", за информационную поддержку при создании книги;

Потий Александру Владимировичу, кандидату технических наук, преподавателю Харьковского Государственного университета радиоэлектроники;

Соснину Александру Васильевичу, кандидату технических наук, доценту, заместителю директора Института стратегических исследований, руководителю Центра информационных ресурсов и технологий;

Тандуре Сергею Владимировичу, директору ООО "D.A.S.";

Чарчиян Светлане Петровне, литературному редактору, за проявленные терпение, выдержку и тактичность в процессе исправления многочисленных ошибок и неточностей, допущенных мною в рукописи;

Шпаку Юрию Ивановичу, кандидату технических наук, начальнику отдела Киевского международного университета гражданской авиации;

Отдельная благодарность

Андрею Непомнящему молодому и талантливому художнику за прекрасные карикатуры, которые создают хорошее настроение при работе с книгой;

Дмитрию Домареву за помощь в подборе подписей для карикатур.

О книге

В книге рассматриваются актуальные вопросы создания систем защиты информации в условиях полной открытости современных информационных технологий.

Согласитесь, что с одной стороны защита информации – это наука, а с другой – искусство! Как объединить эти понятия в нечто логическое целое и стоит ли вообще этим заниматься?

Это издание задумано не для того, чтобы поведать о существовании разнообразных средств и способов защиты информации, коих бесчисленное множество и о которых уже сказано достаточно много. Не хотелось бы утомлять читателя дальнейшим углублением в дебри подробностей, этим успешно занимаются другие.

Направленность книги — не в глубины знаний, а к их вершинам. Попробуйте взглянуть на проблему не с низу, а сверху, и тогда станет понятным многое из того что сейчас делается у основания пирамиды информационной безопасности...

Задача, поставленная автором, состоит не в описании новых сведений о вопросах обеспечения безопасности информационных технологий, а в их систематизации. Необходимо что бы каждый кирпич приобретенных знаний укладывался в стройную архитектуру строящегося здания без лишних затрат и последующих переделок.

В данном случае не стоит вникать в тонкости функционирования тех или иных конкретных механизмов защиты информации. Постарайтесь выяснить как они взаимодействуют друг с другом! Задумайтесь над тем какая роль отведена каждому из них в общей структуре СЗИ. И если при этом Вам пригодится подход к решению указанной проблемы, изложенный в этой книге, то можно считать, что силы и время, потраченные автором, не пропали зря.

Повод для написания

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, преложенный 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.

Источники информации...

Основная работа над книгой заключалась в подборе и обобщении уже имеющихся публикаций по указанной тематике. В частности, в книге использованы материалы таких признанных авторов, как: Безруков Н.Н., Гайкович В.Ю., Галатенко В.А., Герасименко В.А., Демченко Ю.В., Карпов А.Г., Лукацкий А.В., Першин А.Ю., Размахнин В.К., Самохин Ю., Сталенков С.Е., Шепелявый Д., Шураков В.В. и многие другие.

Кроме того, приводятся материалы, подготовленные специалистами таких известных фирм, как:

- Информзащита (Россия),
- Лаборатория ППШ (Россия),
- АО "Инфосистемы Джет" (Россия),
- D.A.S. (Украина),
- Бартек (Украина),
- и др.

Информационную поддержку в процессе подбора материалов для книги осуществлял один из ведущих провайдеров Internet в Украине ООО "ElVisti".

В книге использованы рисунки Андрея Непомнящего, а также карикатуры Кособукина Ю., Федько С. Чернявского Г. из сборника анекдотов и карикатур "Ну просто анекдот!" (Издатель "Рабочая газета" с участием фирмы "АВК-пресс").

Над материалами книги работали

Ананский Евгений Викторович, заместитель директора ООО "КВИРИН", предоставил материалы описывающие источники утечки информации по техническим каналам, а также методы выявления закладных устройств (глава 10 "Техническая защита информации на объектах ИС").

Ворожко Валерий Павлович, сотрудник СБ Украины, предоставил материал под названием "Определение сведений, составляющих конфиденциальную информацию предприятия" (глава 17).

Герасимов Борис Михайлович, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, оказал неоценимую помощь в написании главы 6 "Математические модели систем и процессов защиты информации" и главы 25 "Модель комплексной оценки СЗИ".

Голуб Виктор Анатольевич, кандидат технических наук, сотрудник Центрального научно-исследовательского института вооружения и военной техники ВС Украины, принимал непосредственное участие в подготовке материалов главы 25 "Модель комплексной оценки СЗИ".

Качко Елена Григорьевна, профессор кафедры программного обеспечения ЭВМ Харьковского Государственного университета радиоэлектроники, специалист в области системного программирования и разработки программных систем защиты информации. Ею подготовлен материал по вопросам защиты электронной почты, (глава 14 "Защита каналов связи").

Короленко Михаил Петрович, начальник центра технической защиты информации ОАО "КП ВТИ" описал архитектуру подсистемы защиты информации в АС (глава 26).

Потий Александр Владимирович, кандидат технических наук, преподаватель Харьковского Государственного университета радиоэлектроники, специалист в области криптографических средств защиты информации. Он подготовил интересный материал, описывающий хеш-функции, цифровые подписи и механизмы неотказуемости, (глава 9 "Программно-технические методы и средства защиты информации")

Савчук Александр Менеджер LAN компании Reichle & De-Massari Ukraine подготовил материал "Проблемы технической защиты информации и электромагнитной совместимости для структурированных кабельных сетей" (глава 26).

Татуян Алексей (Semantec Ukraine), подготовил материал "Комплексная стратегия информационной защиты предприятия" (глава 26).

Структура содержания книги

Часть 1 Позвольте Вас познакомить

В этой части книги читатель знакомится с общими проблемами обеспечения безопасности информационных технологий.

Часть 2 Основы построения систем защиты информации

Теоретические основы построения систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.

В этой части книги рассматриваются следующие *ОСНОВЫ* построения систем защиты информации:

- Законодательная, нормативно-методическая и научная база;
- Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации;
- Организационно-технические и режимные меры (политика информационной безопасности);
- Программно-технические методы и средства защиты информации.

Целевая установка теоретических основ заключается в разработке и научном обосновании принципов и методов оптимизации мероприятий по ЗИ. Основной способом достижения указанной цели заключается в решении следующих задач:

- создание предпосылок для реализации упреждающей стратегии ЗИ;
- разработка регулярных методик оценки уязвимости информации и требуемого уровня ее защиты; синтеза оптимальных систем ЗИ;
- обоснование необходимой инфраструктуры ЗИ в общегосударственном масштабе.

Часть 3 Направления создания систем защиты информации

Большое число различных компонентов, операций, ресурсов и объектов ИС создает весьма привлекательную среду для различного рода вторжений и несанкционированных операций.

В этой части книги ИС как объект защиты рассматривается по следующим направлениям:

- Защита информационных и физических объектов информационных систем;
- Техническая защита информации на объектах ИС;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

Рассматривая ИС как объект защиты, обращается внимание на следующие характеристики, влияющие на безопасность информации:

- категории обрабатываемой в ИС информации, высший гриф секретности информации;
- общая структурная схема и состав ИС (перечень и состав оборудования, технических и программных средств, пользователей, данных и их связей, особенности конфигурации и архитектуры и т.п.);
- тип ИС (одно- либо многопользовательская система, открытая сеть, одно- либо многоуровневая система и т.п.);
- объемы основных информационных массивов и потоков,
- спроизводительность системы при решении функциональных задач,
- процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.;
- технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами ИС и пользователями и т.п.);
- территориальное расположение компонентов ИС, их физические параметры и т.п.;
- наличие особых условий эксплуатации и др.

Часть 4 Этапы создания систем защиты информации

В этой части рассмотрены следующие ЭТАПЫ создания СЗИ:

- 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.

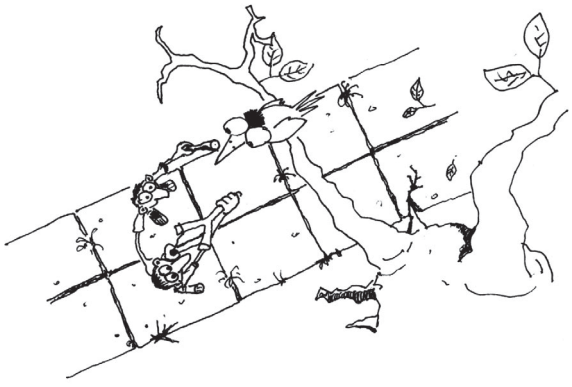
Часть 5 Конкретные решения и рекомендации…

В этой части книги приводятся описания конкретных подходов, разработок и изделий различных фирм и организаций, работающих в области проблем защиты информации.

Как работать с книгой

Многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. Большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том как же приступить к созданию комплексной системы защиты информации для конкретных информационных систем, с учетом присущих им особенностей и условий функционирования.

Вместе с тем, в настоящее время разработано и применяется достаточное количество технологий, способов и средств защиты информации, которые необходимо проанализировать и использовать уже сегодня. Это позволит резко сократить вероятность утечки сведений конфиденциального характера. Но как сложить в стройную систему разрозненные знания и частные решения?



Надо быть выше и немного в стороне…

Нам сверху видно все...

Как известно, для того чтобы решить проблему надо быть выше нее и немного в стороне. Итак попробуем взглянуть на проблему сверху и охватить все ее аспекты. Обратите внимание на рисунок 1.

Известно, что ОСНОВОЙ или составными частями практически любой СИСТЕМЫ (в том числе и системы защиты информации) являются:

1. Законодательная, нормативно-правовая и научная база;
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
3. Организационно-технические и режимные меры и методы (политика информационной безопасности);
4. Программно-технические способы и средства.

Представим ОСНОВЫ в виде куба, внутри которого и находятся все вопросы (предметная область) защиты информации (Рис.2).

Далее, руководствуясь принципом “разделяй и властвуй”, выделим основные НАПРАВЛЕНИЯ в общей проблеме обеспечения безопасности информационных технологий (они представлены на Рис. 3).

НАПРАВЛЕНИЯ формируются исходя из конкретных особенностей ИС как объекта защиты. В общем случае, исходя из типовой структуры ИС и исторически сложившихся видов работ по защите информации предлагается рассмотреть следующие направления:

1. Защита объектов информационных систем;
2. Защита процессов, процедур и программ обработки информации;
3. Защита каналов связи;
4. Подавление побочных электромагнитных излучений.
5. Управление системой защиты;

Но поскольку каждое из этих направлений базируется на перечисленных выше ОСНОВАХ, то грани куба объединяют ОСНОВЫ и НАПРАВЛЕНИЯ неразрывно связанные друг с другом (см. Рис. 3).

Но это еще не все... Далее рассматриваются ЭТАПЫ (последовательность шагов) построения СЗИ (см. Рис. 4), которые необходимо пройти в равной степени для всех и каждого в отдельности НАПРАВЛЕНИЙ (с учетом всех ОСНОВ).

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

1. Определение информационных и технических ресурсов, а также объектов ИС(!) подлежащих защите;
2. Выявление полного множество потенциально возможных угроз и каналов утечки информации;

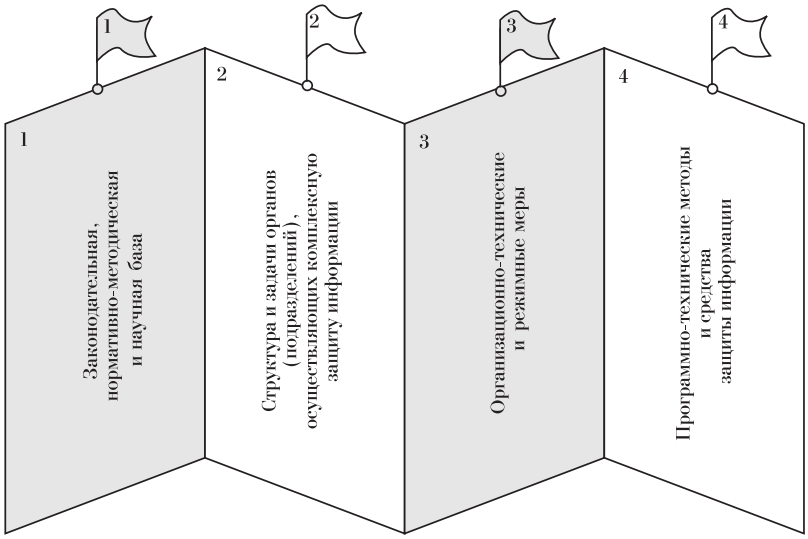


РИСУНОК 1. *Основы*

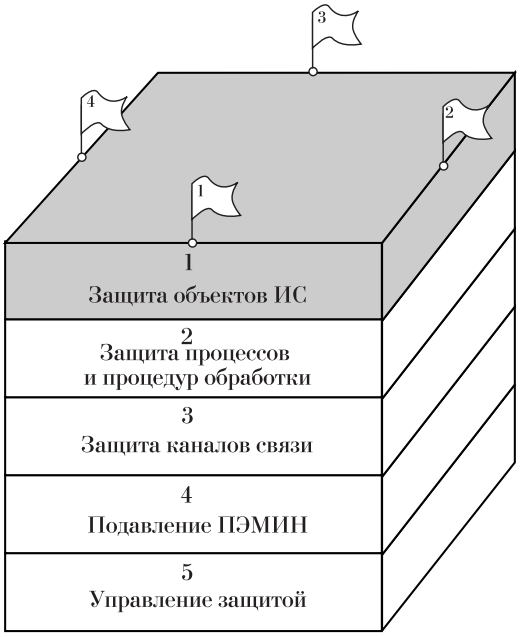


РИСУНОК 2. *Основы*

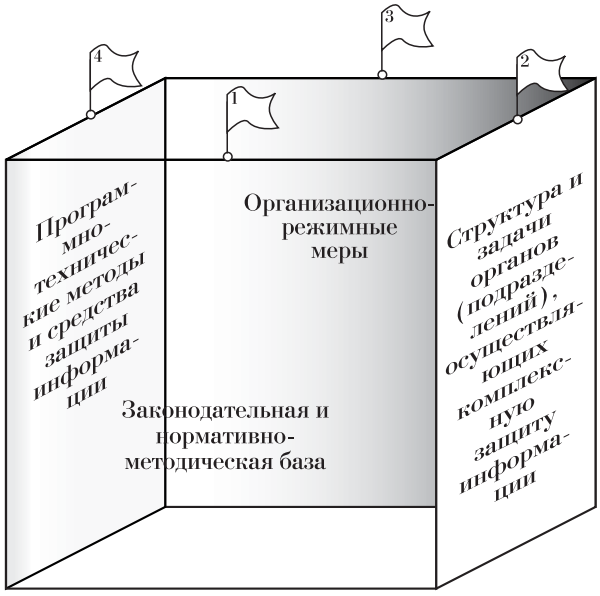


РИСУНОК 3. *Направления*

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

4. Определение требований к системе защиты информации;

5. Осуществление выбора средств защиты информации и их характеристик;

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

7. Осуществление контроля целостности и управление системой защиты.

Указанная последовательность действий осуществляется непрерывно по замкнутому циклу, с проведением соответствующего анализа состояния СЗИ и уточнением требований к ней после каждого шага.

Последовательность прохождения ЭТАПОВ создания СЗИ для каждого из НАПРАВЛЕНИЙ с учетом ОСНОВ (общего представления структуры СЗИ) условно показано на Рис. 4.

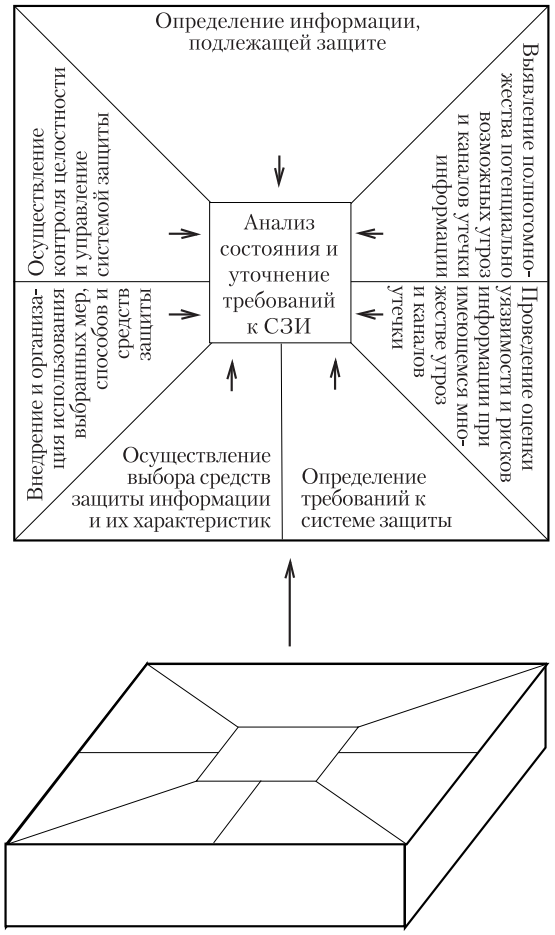


РИСУНОК 4. *Применение МЕТОДИКИ для каждого из НАПРАВЛЕНИЙ с учетом общего представления структуры СЗИ.*

Таким образом получился своеобразный кубик Рубика с взаимосвязанными элементами.

А теперь попробуем развернуть этот кубик на плоскости (на листе бумаги), иначе книга не сможет закрываться. Получится трехмерная матрица или попросту таблица, которая поможет систематизировать материал, изложенный в книге.

Матрица знаний информационной безопасности

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 для этого составляют турнирную таблицу, куда заносятся результаты футбольных игр. При этом после проведения всех встреч команд каждой с каждой, можно сделать вывод об уровне состояния мастерства как команд в целом, так и отдельных игроков.

МАТРИЦЫ СОСТОЯНИЙ –своего рода турнирная таблица, позволяющая логически объединить составляющие блоков “ОСНОВЫ”, “НАПРАВЛЕНИЯ” и “ЭТАПЫ” по принципу каждый с каждым.

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

Наглядно процесс формирования СЗИ с использованием матрицы знаний изображен на Рис. 5.

Рассмотрим как можно использовать предложенную матрицу.

Элементы матрицы имеют соответствующую нумерацию (см. Рис.6.) 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”.

Такая же нумерация используется в названиях разделов, глав и вопросов, рассматриваемых в книге.

В общем случае количество элементов матрицы может быть определено из соотношения

$$K = O_i * H_j * M_k$$

где

K – количество элементов матрицы

O_i – количество составляющих блока “ОСНОВЫ”

H_j – количество составляющих блока “НАПРАВЛЕНИЯ”

M_k – количество составляющих блока “ЭТАПЫ”

В нашем случае общее количество элементов “матрицы” равно 140

$$K = 4*5*7 = 140.$$

поскольку $O_i = 4$, $H_j = 5$, $M_k = 7$

Представление элементов матрицы

Содержание каждого из элементов МАТРИЦЫ описывает взаимосвязь составляющих создаваемой СЗИ. Перечень вопросов описывающих каждый из элементов матрицы, приведен в приложении А.

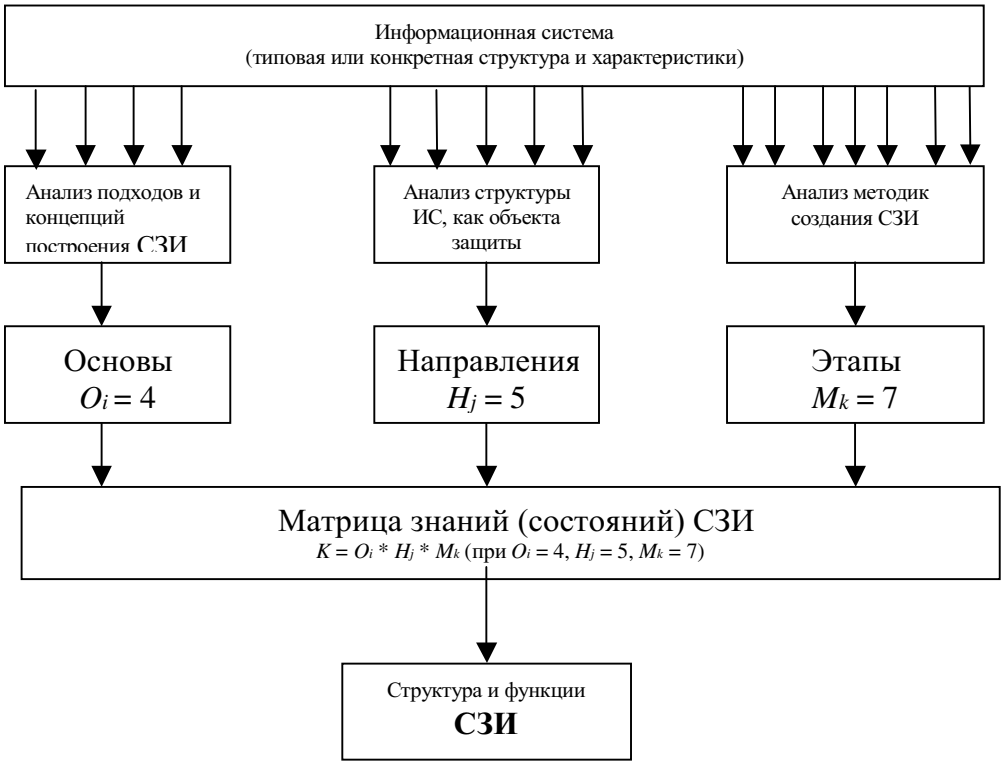


РИСУНОК 5. *Структурная схема формирования СЗИ с помощью матрицы знаний.*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 6. *Нумерация элементов матрицы знаний.*

Комплекс вопросов создания и оценки СЗИ рассматривается путем анализа различных групп элементов матрицы, в зависимости от решаемых задач.

Например отдельно можно оценить ***качество нормативной базы*** (Рис.7) или ***защищенность каналов связи*** (Рис.8), или ***качество мероприятий по выявлению каналов утечки информации*** (Рис.9) и т.д.

В общем случае основным содержанием элементов матрицы является ответ на вопрос “Какие из мероприятий по защите информации, кем и как выполняются?”

В другом примере на Рис.10 приведено содержание для элементов № 321, 322, 323, 324, которые объединяют следующие составляющие:

<<< Этапы	Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 7

<<< Этапы	Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 8

<<< Этапы	Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 9

<<< Этапы	Направления >>>	010 Защита объектов ИС				020 Защита процессов и программ				030 Защита каналов связи				040 ПЭМИН				050 Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИСУНОК 10

- № 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”.

Опишем содержание информации в указанных элементах матрицы.

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). Описание этих вопросов позволяют составить полное представление о СЗИ и оценить достигнутый уровень защиты.

Полный перечень 140 вопросов изложен в Приложение А.

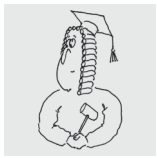
И еще...

Поскольку “от корки до корки” книгу никто читать не станет, то для удобства поиска нужной информации в книге используются пиктограммы, привлекающие внимание читателя.

На пиктограммах изображены:

Руководитель службы безопасности фирмы или администратор безопасности компьютерной сети

Программист или администратор компьютерной сети



Юрист

Злоумышленник

Хакер или недисциплинированный программист

Руководитель фирмы или организации

Пиктограммы сопровождаются комментариями:

Совет,	*Надо знать,*	*Это важно,*
Факты,	*Интересно,*	*Определение,*
Пример,	*Кстати,*	*Юмор*

Попробуйте определить необходимую Вам информацию в предложенной классификации. Удачи Вам, и хорошего настроения при чтении книги.