УДК 681.31

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ СОЗДАНИЯ И ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

А.А.АБДУЛАЕВ, Н.А.ТЮМЕНБАЕВА, Ж.С.ОМУРЗАКОВА
E.mail. ksucta@elcat.kg

Макалада маалыматты коргоонун натыйжалуулугун баалоодо системалык ыкмасы каралган. Маалымат коопсуздугунун моделин түзүүнүн жолдору жана моделде талаптар көрсөтүлгөн. Маалыматтардын коргоо системалардын натыйжалуулугун баалоо усулдары келтирилген.

В статье описывается системный подход к оценке эффективности систем защиты информации. Описываются требования к модели и подход к формированию модели ИБ. Приводится методика оценки эффективности системы защиты информации.

The article describes a system approach to an assessment of efficiency of information security systems. And the Requirements approach of model to formation and Information Security. It will be brought a technique of an assessment of system and a effectiveness of information security.

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 /1/.

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 ближайшее время придется жить в обществе (среде) информационных технологий, куда направлены 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 неэффективно.

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

СЗИ лишь тогда станет системой, когда будут установлены логические связи между всеми ее составляющими.

Для решения вопросов взаимодействия нужно перейти от "чисто" технического на "конкретно" логический уровень представления процессов создания и функционирования систем защиты информации /2/.

Таким образом, многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них.

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 /3/. В упрощенном виде модель СЗИ представлена на рис. 1.

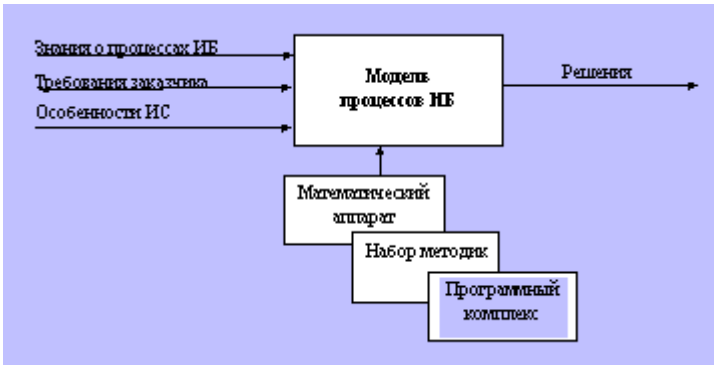

Рис. 1. Модель СЗИ

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/4/:

- 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 (методики) оценки СЗИ;
- модели СЗИ для проведения исследований (матрицы состояния).

Обладать свойствами:

- универсальностью;
- комплексностью;

- простотой использования;
- наглядностью;
- практической направленностью;
- быть самообучаемой (возможностью 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.

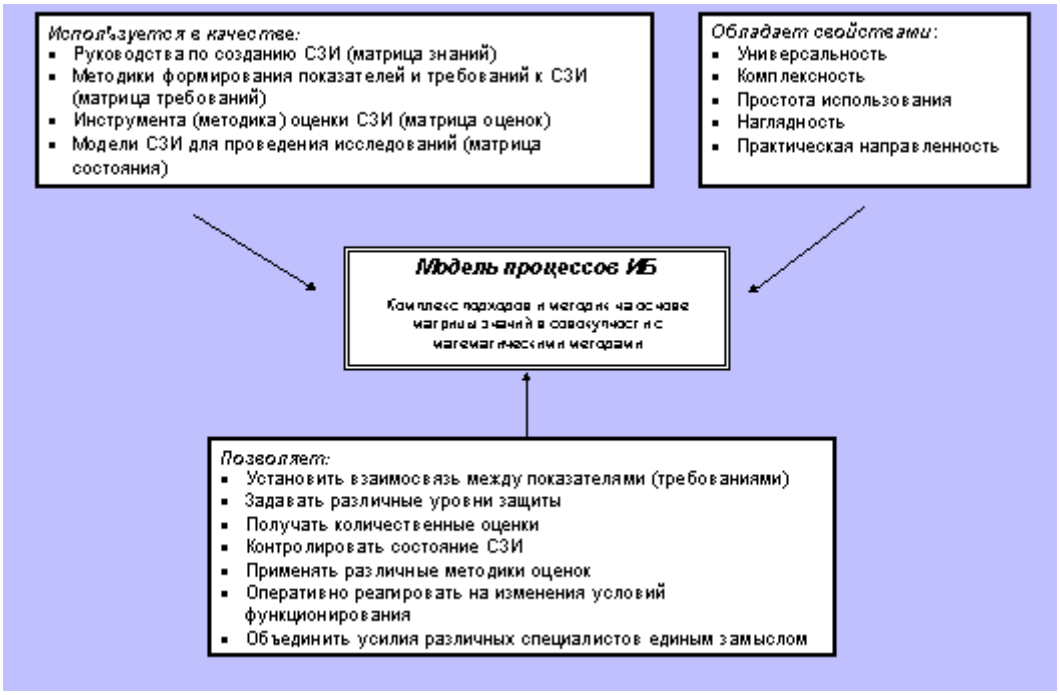

Рис. 2. Требования к модели СИЗ

Описание подхода к формированию модели ИБ

Для охвата всех аспектов информационной безопасности необходимо рассмотреть ее трехмерную модель: Составными частями практически любой сложной 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.

В общем случае, учитывая типовую структуру ИС и исторически сложившиеся виды 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 элементы основ и направлений рассматриваются неразрывно друг с другом.

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 /1-5/:

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

2. Выявление полного множества потенциально возможных угроз и каналов утечки информации.

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.

Оценка эффективности систем защиты информации

С целью реализации модели СЗИ, представленной в виде трехмерной матрицы, и демонстрации преимуществ системного подхода к созданию и оценке эффективности систем защиты информации разработана Программа "Оценка СЗИ" /5/.

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.

Список литературы

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

2. Кульгин М. Технологии корпоративных сетей: Энциклопедия. – СПб.: Питер, 2000. – 704 с.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2001. – 672 с.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – 2-е изд. – М.: Радио и связь, 2002. − 328 с.

5. **http://www.citforum.ru/security/articles/model_proc/** Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации.