5) определение отношений между множествами ДФ, уязвимостей и угроз.

Для формирования множеств сущностей, фигурирующих в процессе реализации угрозы, необходимо выбрать удобную для представления этих множеств классификацию. При этом целесообразно учитывать специфику конкретной ИТС и отдавать предпочтение наиболее актуальной классификации. Модель угроз представляется в виде таблицы, которая также может сопровождаться таблицами, характеризующими множества сущностей, содержащихся в модели угроз, и снабженных соответсвующими идентификаторами.

Таблица – Пример обобщенной модели угроз в ИТС

№ п/п	Название и тип угрозы	Субъект угрозы	Объект угрозы	Возможная атака	ДФ	Используемая уязвимость
1	$T_l(\tau)$	$S_m(\tau)$	$O_n(\tau)$	$A_i(\tau)$	$D_j(\tau)$	$V_k(\tau)$

V Выводы

Предложенные соображения позволяют существенно упростить процесс построения модели угроз при создании защищенных ИТС. В частности, приведенный подход:

- инвариантен относительно применения к разным классам и типам ИТС;
- позволяет описать любую реальную ситуацию;
- является открытым, поскольку предусматривает добавление новых сущностей;
- учитывает любые классификации входящих сущностей.

Однако, формальное описание рассматриваемых множеств может быть неоднозначным, так как на практике зачастую сложно определить четкую грань между понятиями ДФ, уязвимости и угрозы. Кроме того, данный подход изначально не предполагает возможности построения универсальной модели угроз, поскольку все возможные угрозы перечислить невозможно вследствие появления новых, возникающих по мере развития технологий. Поэтому приоритетной задачей эксперта в сфере безопасности информации при разработке модели угроз является выделение наиболее существенных угроз для конкретной ИТС.

Литература: ***1****. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1–003–99, ДСТСЗІ СБ України, Київ, 1999. – 26 с..* ***2****. Антонюк А. О., Жора В. В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 2 - К.:2001, с. 42-46.* ***3****. Сердюк В. А. Классификация угроз информационной безопасности сетей связи, их уязвимостей и атак нарушителя. // Информационные технологии, № 9. - М.:2002, с. 7-12.* ***4****. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат.-1994.-тт.1, 2.* ***5****. А. А. Антонюк, Е. Н. Боровская, В. Ю. Суслов Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. – № 2. – 2001. – 17-22 с.* ***6****. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999. – 16 с.* ***7****. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Изд. Молгачева С. В., 2001. – 352 с.* ***8****. Антонюк А. О., Жора В. В. Моделювання доступу та каналів витоку в інформаційних системах. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 3 - К.:2001, с. 156-160.*

УДК 681.3

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ. ФОРМАЛЬНЫЙ ПОДХОД

Игорь Павлов
ВИТИ НТУУ «КПИ»

Анотация: **Раскрывается понятие процесса проектирования систем защиты информации и дано его математическое описание.**

Summary: **In article the concept of process of systems designing of information protection is opened, and its mathematical description is given.**

*Ключевые слова: П***роектирование систем защиты информации.**

I Введение

Существующие нормативные документы по оценке защищённости определяют гарантии безопасности,

в которых проектирование и разработка систем защиты информации рассматриваются как основные требования безопасности [1]. При высоких требованиях безопасности, предъявляемых к системам защиты информации (для систем государственного назначения, банковских систем), в нормативных документах предписывается к разработчикам обязательная формализация всех этапов создания систем защиты информации (СЗИ).

В настоящей статье даётся определение понятия процесса проектирования систем защиты, а также предложен системный подход в формализации процесса проектирования СЗИ, определены свойства процесса проектирования.

II Основная часть

Задачи проектирования (СЗИ) принципиально отличаются от задач проектирования иных информационных систем. Проектирование осуществляется с учётом статистических данных об уже существующих угрозах. Однако в процессе функционирования системы защиты поле угроз может принципиально измениться. В частности, это связано с тем, что многие угрозы предполагают нахождение злоумышленниками ошибок в реализации системных средств, которые могут быть неизвестны на момент создания системы защиты, но должны быть учтены в процессе её функционирования.

Процесс проектирования систем защиты информации (СЗИ) можно представить в виде спирали, где каждый новый виток определяет новые требования к проектированию на основе новых угроз систематизированных в процессе функционирования СЗИ, и предполагаемых угроз, которые могут возникнуть при новой доработке системы. Место проектирования в жизненном цикле СЗИ представлено на рис. 1. Поэтому проектирование системы защиты – процедура итерационная, в общем случае предполагающая следующие этапы:

1. проектирование первоначальной системы защиты (раннее проектирование);
2. разработка эскиза модели СЗИ;
3. проведение испытаний (моделирование ситуаций, испытания аппаратуры);
4. анализ защищенности на основе статистических данных, полученных в процессе функционирования системы защиты;
5. модификация «узких мест» системы защиты на следующем «витке» проектирования системы защиты.

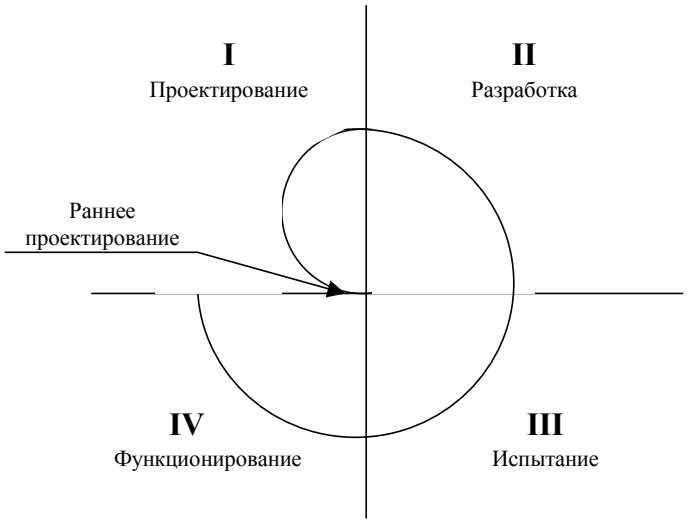

Рисунок 1 – Жизненный цикл СЗИ

В свою очередь для этапов проектирования свойственны три основных подхода к построению СЗИ, показанных на рис. 2.

1. Разработка и внедрение новых систем, в рамках которых решается весь комплекс защиты информации (креативный подход).
2. Модификация существующих информационных систем с целью дополнения их функциями защиты информации (аддитивный подход).

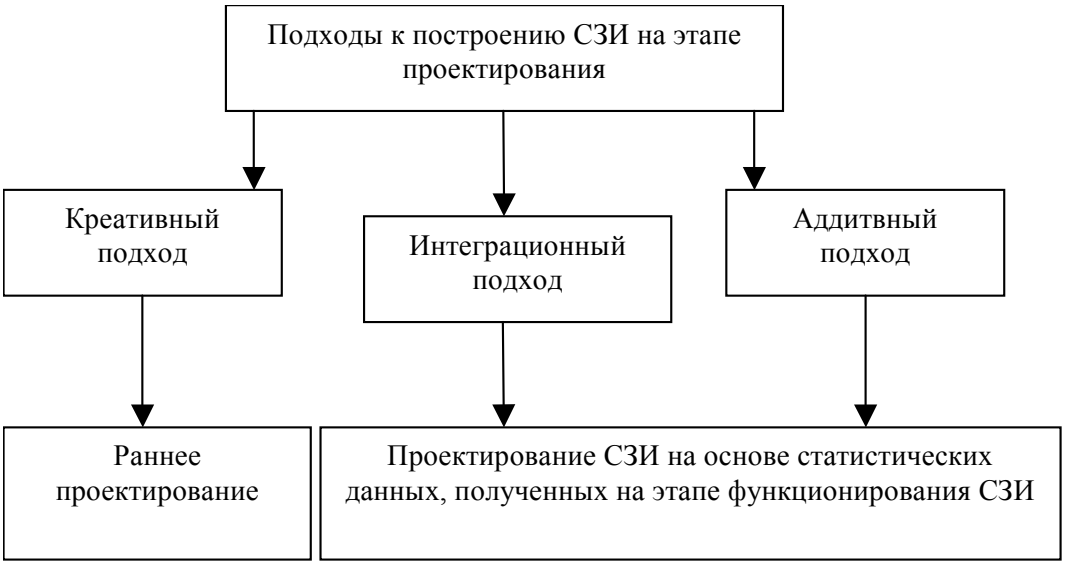

Рисунок 2 – Подходы к построению СЗИ на этапах проектирования

3. Разработка подсистем защиты информации, решающих отдельные задачи обеспечения безопасности, и их интеграция в существующие информационные системы (интеграционный подход).

Креативный подход предлагает наиболее радикальный способ решения проблемы защиты информации. Однако построение сложной информационной системы «с нуля» требует больших временных и финансовых затрат. Такой подход свойственен для создания СЗИ государственного значения.

Вследствие недостатков креативного подхода широкое распространение получил аддативный подход к построению СЗИ. Применение данного подхода позволяет сократить время на разработку защитной системы за счёт использования готовых средств. Однако, анализ существующих разработок на основе аддативного подхода показывает высокую уязвимость подобных систем [2]. Это в частности связано с многовариантностью путей обмена информацией, что не позволяет обеспечить надёжный контроль над всеми информационными потоками. Такой подход свойственен для коммерческих систем.

Интеграционный подход является развитием этих двух подходов. При использовании интеграционного подхода в отличии от креативного система создаётся не «с нуля», а строится на основе готовых блоков интеграции, что заметно снижает трудоёмкость разработок.

Для определения единой методологии подходов к решению проектных задач создания СЗИ на различных уровнях проектирования необходимо формализовать понятие процесса проектирования систем защиты информации. До настоящего времени понятие «объекта – проектирования» и «процесса – проектирования» определялось на интуитивном уровне. Попытки их формализации предпринимались в работе [3,4], однако их нельзя считать завершёнными.

Под проектированием понимается процесс создания технической документации, необходимой для изготовления и эксплуатации некоторого объекта. Такое определение принято для классической системотехники [5], оно неформально, и скорее поясняет цель проектирования, а не суть соответствующего процесса проектирования СЗИ. Частично формализовать это понятие можно определив модель объекта проектирования, процедуру работы с этой моделью и понятие оптимальности проектного решения.

Пусть объект проектирования (ОП) характеризуется тройкой вида:

$$\text{ОП} = \{F, S, P\} \qquad (1)$$

где F, S, P – соответственно функциональное, структурное и параметрическое описание объекта.

Функциональное описание отражает траекторию ОП в пространстве время – состояние как некоторую функцию, аргументами которой являются управляющие воздействия и пассивные воздействия внешней среды. Управляющие воздействия могут быть как внешними, так и внутренними.

Если объект с заданным F – описанием или документация, по которой он может быть создан, существует, то задачу проектирования решать не имеет смысла при условии, что параметрическое описание удовлетворяет техническим требованиям. В противном случае такой объект необходимо проектировать. В процессе проектирования обычно используются приёмы, связанные с декомпозицией F – описания [6] на некоторые подфункции:

$$F = S(F_i), \quad i = \overline{1,n}, \tag{2}$$

где S – оператор, определяющий такую комбинацию F_i, которая обеспечивает исходное F – описание. S – оператор в дальнейшем будем называть структурным описанием системы (S - описанием), которая и задаёт структуру ОП на рассматриваемом уровне детализации.

Некоторой части из полученных в результате декомпозиции F, могут соответствовать известные объекты, которые называются элементами. Элемент может быть достаточно сложной технической системой. Существенным в этом случае является то, что F – описание элемента не требует дальнейшей декомпозиции и, следовательно, он не имеет S – описания.

Для оставшейся части F вновь необходима декомпозиция, и так до тех пор, пока все F – описания не будут соответствовать элементам. Таким образом:

$$F_i = S(F_{i+1}, j), \quad i = \overline{1,m}, \quad j = \overline{1,n_i}, \tag{3}$$

где i – определяет номер шага, j – индекс компонента на соответствующем шаге. Процесс декомпозиции F – описаний не однозначен, причём множество допустимых решений достаточно велико. Выбор варианта декомпозиции обычно определяется качеством полученного решения.

Пусть качество есть множество свойств ОП [7], имеющих количественное выражение и называемых параметрами $P = \{p_i\}, \quad i = \overline{1,k}$. Тогда p_i – описание есть:

$$p_i = \Phi(p_{i+1}), \tag{4}$$

где Ф – оператор, задающий соответствие между P и параметрами следующего уровня p_i , причём F – описанию всегда ставится соответственно P – описание.

Используя предложенную модель ОП и интерпретируя процесс проектирования граф деревом, получим, что вершиной графа является тройка: (F_0,S_0,P_0), где:

$$F_0 = S_0(f_{1,i}), \tag{5}$$

$$P_0 = \Phi_0(p_{1,i}). \tag{6}$$

На следующих уровнях

$$F_i = S_i(f_{i+1,j}), \tag{7}$$

$$P_i = \Phi_i(p_{i+1,j}), \tag{8}$$

причём S и Ф определяются после очередного шага декомпозиции.

Таким образом, оператор Ф связывает параметры только двух смежных уровней и представляет собой систему уравнений вида:

$$\begin{aligned} p_1 &= f_1(x_1, x_2, \ldots, x_q) \\ p_i &= f_i(x_1, x_2, \ldots, x_q), \\ p_k &= f_k(x_1, x_2, \ldots, x_q) \end{aligned} \tag{9}$$

где p_i – элемент множества P (верхний индекс не конечен), а аргументами функций являются параметры, соответствующие P – описанию следующего уровня. Однако при решении практических проектных задач система (9) должна быть преобразована в систему неравенств, так как значения параметров P - описания обычно задаются в виде допустимых границ. В общем случае односторонние ограничения типа «не более» или «не менее» не нарушают общность преобразования и система (9) сводится к виду:

$$\begin{aligned} a_1 < p_1 &= f_1(x_1, x_2, \ldots, x_q) < b_1 \\ a_i < p_i &= f_i(x_1, x_2, \ldots, x_q) < b_i \\ a_k < p_k &= f_k(x_1, x_2, \ldots, x_q) < b_k \end{aligned} \tag{10}$$

Значения x_i, удовлетворяющие системе (10) ограничивают множество допустимых вариантов решения задачи декомпозиции F – описания на определённом уровне. Любое из этих решений можно считать оптимальным. Для получения строгого оптимального решения по одному или нескольким p_i необходимо ужесточить соответствующие значения a_i и b_i. Если система неравенств не имеет решения, то нужно, наоборот, расширить границы упомянутых значений, то есть искать так называемое квазиоптимальное решение. Стратегия его поиска иллюстрируется геометрической интерпретацией, изображённой на рис. 3.

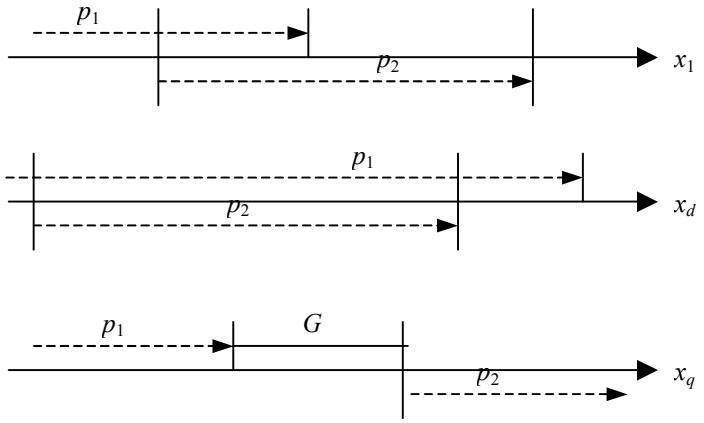

Рисунок 3 – Соотношение вариантов решений поставленных задач и вариантов декомпозиций, определяемых качеством решаемых задач

Пусть выделенные области осей абсцисс соответствуют значениям аргументов x_i, удовлетворяющих решению отдельных неравенств системы (10), в которой для простоты рисунка учтены только 2 параметра. Если на каждой из осей есть общие значения x_i (в примере оси x_1 и x_d) для всех параметров, то решение системы и, следовательно, оптимальная декомпозиция F – описаний на данном уровне возможны. В противном случае, к которому сводится рассматриваемый пример из-за оси x_q , необходимо «стянуть» в точку область, обозначенную на рис. 3 как область G, изменением a_i , b_i .

Стягивание в точку можно осуществить смещением значений аргумента x_i , которое достигается изменением соответствующих ограничений либо для обоих параметров, либо только для одного из них. При этом необходимо помнить, что такие изменения могут влиять на значения остальных аргументов и, следовательно, привести к исчезновению области пересечения на других осях, например x_1, x_d. В этом случае решение задачи декомпозиции при заданном P – описании невозможно в силу противоречивости параметров p_1 и p_2 . Важным дополнением модели процесса проектирования является понятие уровня отрыва. Это понятие соответствует тем уровням декомпозиции, на которых происходит замена математического аппарата или, в общем случае, способа задания F – описаний.

Пусть смежные уровни отрыва выделяют шаги декомпозиции в некотором интервале (r,s), тогда соответствующие им ярусы дерева характеризуются четвёркой (V_p, V_c, PR, PL), где:

- $V_p = \{V_{p_i}\},\ i = \overline{1,n}$ - множество примитивов, элементами которого являются F – описания на S – том уровне графа дерева.
- $V_c = \{V_{c_i}\},\ i = \overline{1,m}$ - множество конструкций, элементы которого соответствуют F – описанию на r, … , S-1 шагах.
- $PR = \{pr_i\},\ i = \overline{1,k}$ - множество допустимых правил с помощью которых могут быть заданы отражения $V_p \times V_p \to V_c,\ V_p \times V_c \to V_c,\ V_c \times V_c \to V_c$.
- $PL = \{pl_i\},\ i = \overline{1,h}$ - множество локальных параметров, используемых для оптимизации проектных решений на рассматриваемом уровне.

Таким образом, уровни отрыва выделяют так называемые уровни проектирования [3, 8 – 11], например, при проектировании СЗИ различают системный, операционный, функционально-логический, схемотехнический и конструктивно-технический уровни [12].

Важным следствием сказанного выше является утверждение о том, что используемые в пределах одного уровня методы решения проектных задач ограничены допустимыми примитивами V_p и множеством PR.

Используя предложенную модель процесса проектирования можно формально определить ряд понятий, связанных с методологией проектирования, в частности, как нисходящее (сверху - вниз) и восходящее (снизу - вверх) проектирование.

Нисходящее проектирование в соответствии с моделью является приёмом поиска решения в случае, когда существует детерминированная процедура декомпозиции F – описания на всех уровнях. Однако для большинства реальных проектных задач такая процедура известна не на всех уровнях. Тогда решение задачи декомпозиции на этих уровнях сводится к попытке получить, с помощью некоторого набора подфункций $F_{i,j}$, исходное F – описание эвристическими методами, то есть снизу – вверх (оба вида

процедур назовём решением задачи синтеза). Необходимым и достаточным условием успеха эвристической процедуры является функциональная полнота выбранного набора подфункций.

Сложность эвристической процедуры определяется как сложность генерации очередного варианта *S* – описания, так и количеством возможных вариантов таких описаний (см. (1)). Упростить поиск решения снизу – вверх, используя направленный перебор, позволяет анализ соответствующих *P* – описаний, на основе которого можно исключить неперспективные варианты *S* – описаний.

Кроме того, модель позволяет определить область применения рассматриваемых методик. Исследование *P* – описаний с целью определения эвристик обычно называют решением задачи анализа, а последовательное чередование синтеза и анализа с целью получения решения задачи декомпозиции на очередном шаге – методом последовательных приближений [13]. В большинстве случаев нисходящее и восходящее проектирование распространяется на шаги декомпозиции *F* – описания, расположенные между уровнями отрыва. Зависимость *F* – описания от исследования *S* – описания показана в (3), структурное описание объекта проектирования особенно важно во время системного подхода к оценке качественных показателей системы (объекта).

На основании вышеизложенных положений можно сформулировать понятие процесса проектирования систем защиты информации: Проектирование системы защиты информации – это непрерывный процесс, который базируется на количественной и качественной оценках защищённости системы, осуществляемый от момента зарождения системы (первичное проектирование), в течении всего жизненного цикла системы и последующей её модификации (доработки), основанных на непрерывном анализе текущего состояния обеспечиваемого системой уровня защищённости средствами мониторинга с учётом меняющихся угроз.

III Выводы

Неучёт рассмотренных свойств процесса проектирования обычно приводит к несоответствию классификаторов и некорректному сравнению методов решения проектных задач на различных уровнях проектирования СЗИ, неточностям постановки проектных задач, и что самое опасное, к ошибкам, закладываемым в разработку и создание систем защиты информации, что в дальнейшем приводит к нарушениям безопасности информации.

Качественная оценка механизмов защиты системы защиты информации является основной составляющей оценки эффективности при системном подходе (S - описания) к оценке проектируемых систем защиты, что является дальнейшей работой при исследовании процессов построения систем защиты информации.

Литература: ***1.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. // НД ТЗІ 2.5 – 004 – 99. – К.: 1999. – 51 с.* ***2.*** *Краснощёков П. С., Федоров В. В., Морозов В. В. Проектирование технических систем многоцелевого назначения. // «техническая кибернетика». – М.: 1999. – № 4. – С. 68 – 82.* ***3.*** *Майоров С. А., Новиков Г. И. Малогабаритные вычислительные машины. // «Машиностроение». – Л.: 1967. – 236 с.* ***4.*** *Габарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации. // – К.: 2003. – 657 с.* ***5.*** *Холл А. Опыт методологии для системотехники. // – М.: 1975. – 286 с.* ***6.*** *Герасімов Б. М., Домарев В. В. Вибір оптимального варіанту системи захисту інформації на основі застосування методів багатокретеріальної оптимізації. // «Захист інформації». – К.: 2002. – № 3. – С. 24 – 28.* ***7.*** *Капур К. С., Ламберсон Л. А. Надёжность и проектирование систем. // – М.: 1980. – 435 с.* ***8.*** *Бадулин С. С. Автоматизированное проектирование цифровых устройств. // «Радио и связь». – М.: 1980. – С. 57 – 79.* ***9.*** *Батанов Л. А. Автоматизация проектирования цифровых вычислительных устройств. // «Энергия». – М.: 1978. – 356 с.* ***10.*** *Горяшко А. П. Синтез диагностируемых схем вычислительных устройств. // «Наука». – М.: 1987. – 288 с.* ***11.*** *Норенков И. П., Маничев В. Б. Системы автоматизированного проектирования электронно-вычислительной аппаратуры. // «Высшая школа». – М.: 1983. – Вып. 49. – С. 256 - 263.* ***12.*** *Щеглов А. Ю. Защита компьютерной безопасности от несанкционированного доступа. // – С.Пб.: 2004. – 384 с.* ***13.*** *Щеглов А. Ю. Проблемы и принципы проектирования систем защиты информации от НСД. // «Экономика и производство». – М.: 2001. – 03. – С. 34 – 46.*