УДК.681.2

Г.В. Фролов

СИСТЕМНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Предлагается модель системы защиты информационных технологий (ИТ) с использованием сервисов безопасности. Модель выбрана на основе критериев оценки качества систем: критерия пригодности, критерия оптимальности и критерия превосходства на основе предложенной классификации угроз безопасности. Предложенная модель представляет собой совокупность сервисов безопасности, которые могут быть реализованы в среде функционирования ИТ, в самой ИТ или средствами защиты информации.

Введение

Решение задачи создания защищенной ИТ требует от пользователя построения модели угроз для реальной ИТ. Выстраивание же адекватной модели возможно при использовании базы данных угроз безопасности ИТ, содержащей информацию о множестве угроз безопасности ИТ, известных на момент построения защищаемой системы. В настоящее время разработан и поддерживается, в том числе и международными специализированными организациями, ряд таких баз данных. Сравнение содержащихся в существующих базах данных решений показывает значительную разницу как в подходах к классификации угроз, так и в полученных результатах. Необходимо отметить и один общий недостаток – отсутствие системного подхода к решению поставленных задач [1]. Ни в одной из известных баз данных не были использованы системные принципы построения классификации угроз.

1. Выбор варианта реализации системы приемлемого качества

Для выбора варианта реализации системы приемлемого качества применим методологию оценки качества систем.

Критерии оценки качества систем можно разделить на три класса: пригодности, оптимальности и превосходства.

Пусть π_{ij} ($i \in \{1, ..., m\}, j \in \{1, ..., n\}$ – показатель i-го свойства j-й системы, т. е. показатель качества j-й системы есть вектор $\Pi_j = \{\pi_{1j}, \pi_{2j}, \ldots, \pi_{mj}\}$, $\{\pi_{ij}^{(доп)}\}$ – множество допустимых значений показателя π_{ij}. Тогда критерии перечисленных выше классов можно представить следующим образом:

1. Критерий пригодности:

$$K_{приг} : (\bigcup_{i \in M} \{\pi_{ij}\}) \bigcap (\bigcup_{i \in M} \{\pi_{ij}^{доп}\}),$$

где $M=\{1,..., m\}$ – множество всех свойств.

Данное выражение имеет следующий смысл: система j является пригодной по качеству, если значения всех показателей существенных свойств принадлежат допустимым значениям. По этому определению системы, для которых выполняются условия данного выражения, обладают одинаковыми качествами.

2. Критерий оптимальности:

$$K_{опт} : [(\bigcup_{i \in M \setminus M_0} \{\pi_{ij}\}) \bigcap (\bigcup_{i \in M \setminus M_0} \{\pi_{ij}^{доп}\})] \cup [(\bigcup_{i \in M_0} \pi_{ij}\}) \bigcap (\bigcup_{i \in M_0} \{\pi_{ij}^{opt}\})],$$

где M_0 – подмножество оптимальных свойств;

π_{ij}^{opt} – оптимальное значение показателя i-го свойства j-й системы.

Данное выражение имеет следующий смысл: система *j* является оптимальной по m_0 свойствам, если она пригодна по остальным свойствам и показатели свойств из множества M_0 принимают оптимальные значения.

3. Критерий превосходства:

$$K_{прев}:[(\bigcup_{i\in M}\{\pi_{ij}\})\cap(\bigcup_{i\in M}\{\pi_{ij}^{доп}\})]\cap(\bigcup_{i\in M}\left\{\pi_{ij}\,\middle|\,\pi_{ij}\succ\pi_{il}, l\in M, l\neq j\right\}).$$

Данное выражение имеет следующий смысл: система *j* превосходит (обозначение $\succ$) по качеству остальные пригодные системы, если значения показателей ее свойств превосходят либо не хуже значений соответствующих показателей остальных систем.

Если $\pi_{il}=\pi_{ij}$, $i = 1, \ldots, m$, то качества *l*-й и *j*-й систем признаются одинаковыми. Если же хотя бы одно из условий данного выражения не выполняется, то это означает, что заданная совокупность показателей свойств не позволяет выявить систему, превосходящую по качеству все остальные.

Для оценки качества систем необходимо выделить свойства систем (точнее, существенные свойства), отсутствие которых приводит к потере того качества, которое связывалось с безопасностью ИТ. По показателям этих свойств производится оценка качества. Показатель – количественное или качественное выражение свойств системы.

В данной работе предлагается рассматривать следующие существенные свойства:

– типизацию;

– полноту;

– реализуемость.

Для характеристики свойств системы будут использованы показатели, определяющие наличие (отсутствие) существенных свойств.

Одним из вариантов реализации системы безопасности на основе технологии «перекрытия угроз» является непосредственная нейтрализация самих угроз. Это предполагает построение модели угроз, содержащей сведения о всех возможных угрозах (рис. 1).

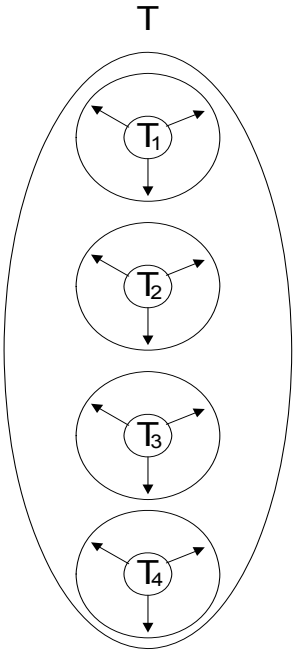

Рис. 1. Модель системы защиты по нейтрализации угроз: T_i – угроза *i*, круг означает операцию нейтрализации

При построении модели угроз разработчик может опираться на нормативные документы, определяющие методологию описания угроз, либо воспользоваться разработанными и поддерживаемыми, в том числе и международными специализированными организациями, базами данных угроз безопасности информации [2–4].

В первом случае количество угроз и их формулировки будут индивидуальными. Во втором случае из-за разницы подходов к классификации и идентификации угроз, которые использованы при разработке баз данных, результаты их применения в каждой конкретной ситуации будут различны, и в этой ситуации нельзя говорить о типовом элементе при построении такой модели системы защиты ИТ.

С одной стороны, при отсутствии нормативно-технической базы, содержащей полный перечень угроз безопасности информации, нет гарантии полноты модели угроз в каждом конкретном случае. С другой стороны, разработчик может включить в модель такое количество угроз, что система защиты станет нереализуемой.

На основании изложенного можно сделать вывод, что вариант реализации системы защиты по принципу нейтрализации угроз является непригодным по качеству, так как в нем отсутствуют свойства типизации и будет отсутствовать либо полнота, либо реализуемость.

Другой вариант реализации системы защиты информации на основе технологии «перекрытия угроз» связан с защитой объектов. В этом случае необходимо построить модель защиты от всех угроз для каждого объекта (рис. 2). При этом разработчик неограничен как в степени детализации объектов, так и в возможности создания новых объектов и выделить типовой элемент защиты не представляется возможным.

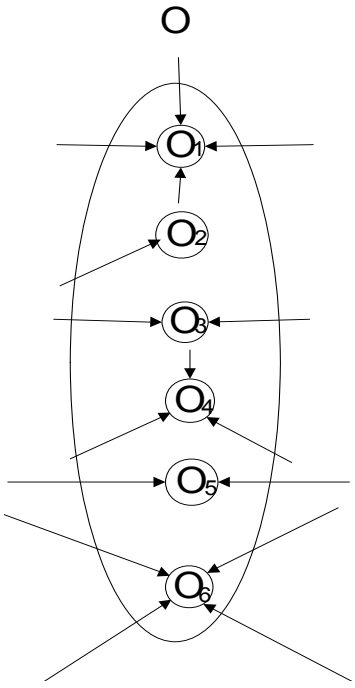

Рис. 2. Модель системы защиты объектов от угроз: O_i – объект *i*

В отсутствие ограничения на число объектов и угроз для каждого объекта система защиты может оказаться практически нереализуемой. Реализация системы защиты только для определенной части объектов и угроз приводит к неполноте защиты. Отсюда можно сделать вывод, что, как и в предыдущем случае, рассматриваемые системы защиты не являются качественными по критерию пригодности.

Третий вариант построения системы защиты связан с полным перекрытием угроз (рис. 3). В этом случае определяется множество угроз и объектов и устанавливаются взаимосвязи (пути доступа) для каждой пары «угроза – объект». Каждый идентифицированный путь доступа угро-

зы к объекту должен быть перекрыт системой защиты. В связи с тем что множество угроз и объектов неопределено, нельзя говорить о типизации таких систем безопасности.

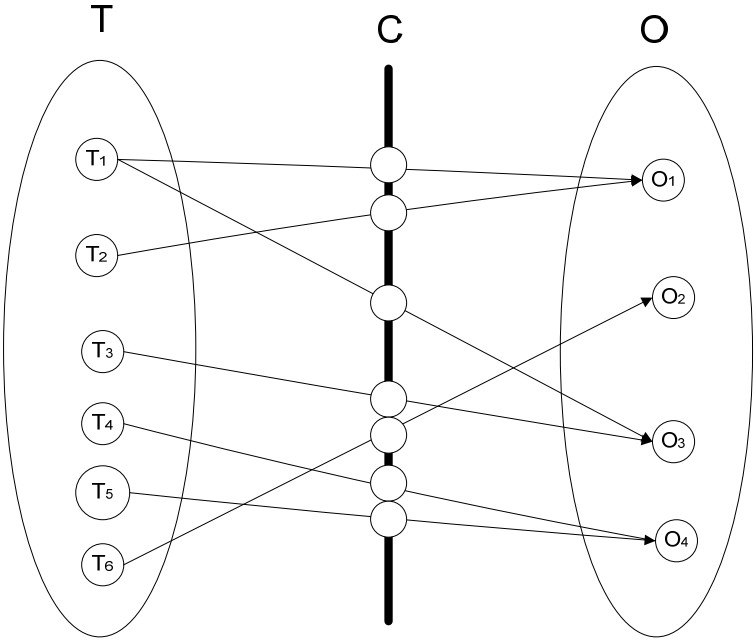

Рис. 3. Модель системы защиты с полным перекрытием угроз: С – перекрытие путей доступа угрозы к объекту

Наличие слишком большого числа взаимосвязей «угроза – объект» в данной модели приведет к ее нереализуемости. Если ограничиться рассмотрением только части взаимосвязей, система защиты будет неполной.

Следствием неопределенности числа угроз и объектов в модели защиты с полным перекрытием является невозможность типизации таких систем защиты и отсутствие реализуемости или полноты защиты. Построенные на основе данной модели системы защиты также не будут пригодными.

Однако для модели систем защиты с полным перекрытием угроз можно достичь определенности объектов защиты и определенности угроз, а при предложенном уровне детализации объектов – полноты защиты. В этом случае обеспечиваются все качественные характеристики системы: типизация, полнота и реализуемость.

2. Классификация угроз безопасности

Описание защищенного состояния системы ИТ S можно представить в виде следующей схемы:

$$S_{ijnm} = \{O_i, T_{ij}, C_{ijn}, F_{ijnm}\},$$

где O_i – множество структурных компонентов ИТ;

T_{ij} – множество угроз i-му структурному компоненту ИТ;

C_{ijn} – множество сервисов безопасности, противодействующих j-й угрозе;

F_{ijnm} – множество требований по реализации n-го сервиса безопасности, противодействующего j-й угрозе на i-й структурный компонент ИТ.

Схема S_{ijnm} может быть достигнута после выполнения цепочки процедур, которые можно представить в виде операторов построения базы данных угроз ($\{T_j, DBJ\} => B_j$), построения модели угроз ($\{S_i, B_j\} => S_{ij}$), разработки системы мер по защите ($\{S_{ij}, B_n\} => S_{ijn}$), построения профиля защиты ($\{S_{ijn}, B_m\} => S_{ijnm}$). Здесь DBJ – инструментарий разработки БД, который должен позволять реализовать БД угроз на основе заданной классификации угроз T_j; B_j – база данных угроз безопасности; B_n – база данных мер противодействия угрозам (сервисов безопасности);

B_m – база данных требований безопасности; S_i – множество структурных компонентов системы; S_{ij} – модель угроз; S_{ijn} – система мер противодействия.

Задача построения защищенной ИТ может быть выражена в виде оператора

$$\{S_i, B_j, B_n, B_m, Z\} => S_{ijnm},$$

где Z – множество задач, которое должно быть решено для того, чтобы реализовать мероприятия по защите.

Каждую угрозу можно рассматривать как процедуру, осуществление которой приводит к ущербу ИТ. Ущерб предлагается выражать в категориях конфиденциальности, целостности и доступности. Кроме того, угрозы можно рассматривать как проявление факторов, воздействующих на защищаемую информацию по ГОСТ Р 51275–99 [5]. Согласно данному стандарту фактор – явление, действие, процесс, результатом которых может быть утечка, искажение, уничтожение, блокирование доступа к информации.

Задача построения таксономии угроз может быть выражена в виде оператора

$$\{S_i, K_{il}, Fa_y\} => T_j,$$

где K_{il} – l-я категория ущерба i-го структурного компонента ИТ;

Fa_y – фактор, воздействующий на информацию.

Данное выражение позволяет сформулировать следующие принципы таксономии угроз:

1. Таксономия угроз должна соответствовать множеству структурных компонентов ИТ.
2. Таксономия угроз должна соответствовать категориям ущерба.
3. Таксономия угроз должна соответствовать таксономии факторов, воздействующих на защищаемую информацию.

Очевидно, что такое представление угроз закладывает возможность при реализации системы обеспечения безопасности ИТ решать задачи контроля:

– возможностей системы защиты по противодействию угрозам на структурные компоненты ИТ;

– возможного ущерба при реализации угроз;

– возможностей системы защиты по противодействию негативному влиянию факторов, действующих на объект информатизации.

3. Разработка баз данных сервисов безопасности и требований безопасности

Задача разработки баз данных сервисов безопасности и требований безопасности может быть сформулирована в виде операторов

$$\{T_n, DBN\} => B_n;$$

$$\{T_m, DBM\} => B_m,$$

где T_n и T_m – заданные классификации сервисов и требований безопасности;

DBN и *DBM* – инструментарии разработки баз данных.

Принципы таксономии сервисов и требований безопасности аналогичны принципам таксономии угроз. Для требований безопасности дополнительно сформулирован еще один принцип таксономии: таксономия требований безопасности должна соответствовать множеству сервисов безопасности. В приложении к разработке базы данных требований безопасности этот принцип означает, что каждому сервису безопасности должно соответствовать множество требований по его реализации.

В качестве инструментариев при разработке баз данных использовались нормативно-методологические документы в области защиты информации [6–11].

В результате проведенных в рамках данной работы исследований был сформулирован следующий принцип: классификация угроз безопасности ИТ должна соответствовать множеству структурных компонентов ИТ и предусматривать наличие атрибутов угроз, указывающих на те структурные компоненты ИТ, в которых угроза может быть идентифицирована.

4. Модель системы защиты ИТ

Таким образом, система защиты ИТ (рис. 4) представляет собой совокупность сервисов безопасности, которые могут быть реализованы:

– в среде функционирования ИТ;

– в самой ИТ (путем использования защитных свойств ИТ);

– средствами защиты информации.

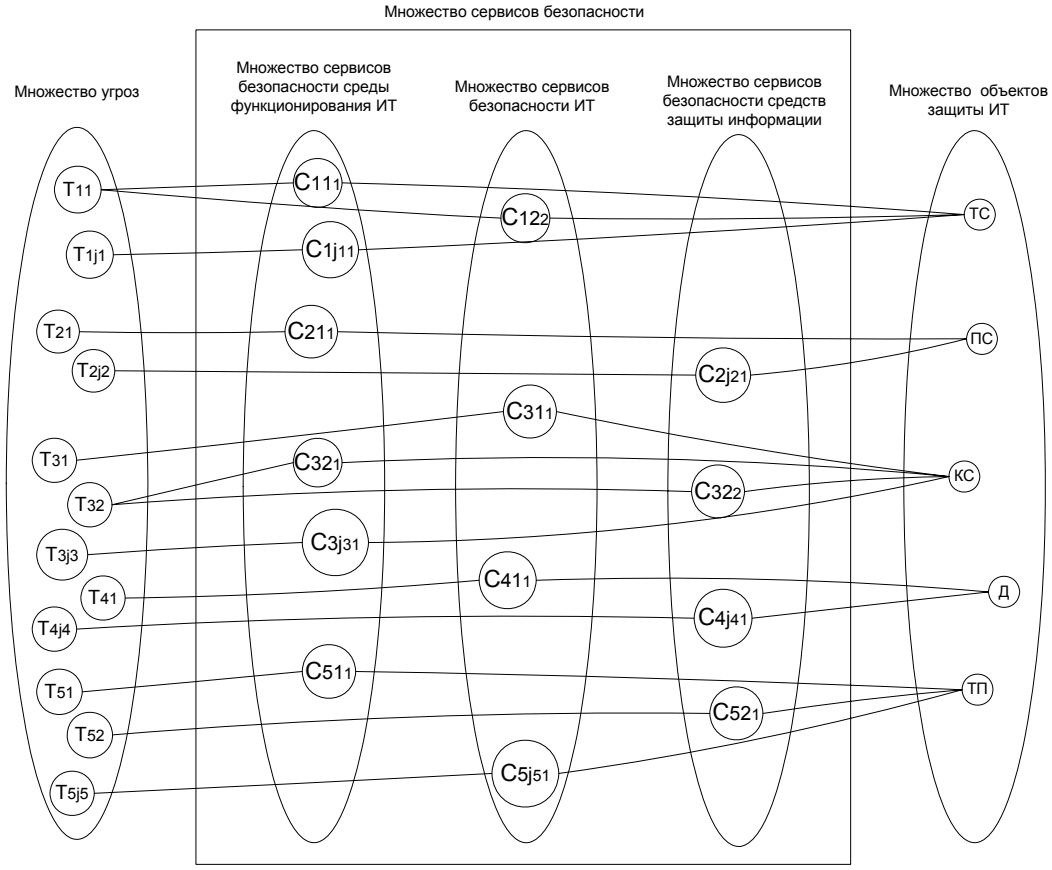

Рис. 4. Модель системы защиты, содержащей три подмножества сервисов безопасности

Модель системы обеспечения безопасности представляет собой трехслойный граф

$$S = \{T, O, C\},$$

где T – множество угроз, $T = \{T_i\}$;

O – множество объектов защищаемой системы, $O = \{O_j\}$;

C – множество сервисов безопасности, $C = \{C_k\}$.

Множество O разбито на взаимно непересекающиеся подмножества

$$O = \{O_1, O_2, O_3, O_4, O_5\},$$

где O_1 – технические средства обработки информации;

O_2 – программные средства обработки информации;

O_3 – каналы связи;

O_4 – данные;

O_5 – технологический процесс.

Множество угроз T разбито на взаимно непересекающиеся подмножества

$$T_1 = \{T_{11}, T_{12}, \dots, T_{1j1}\};$$
$$T_2 = \{T_{21}, T_{22}, \dots, T_{2j2}\};$$
$$T_3 = \{T_{31}, T_{32}, \dots, T_{3j3}\};$$
$$T_4 = \{T_{41}, T_{42}, \dots, T_{4j4}\};$$
$$T_5 = \{T_{51}, T_{52}, \dots, T_{5j5}\},$$

где T_1 – конечное множество угроз техническим средствам обработки информации;

T_2 – конечное множество угроз программным средствам обработки информации;

T_3 – конечное множество угроз каналам связи;

T_4 – конечное множество угроз данным;

T_5 – конечное множество угроз технологическому процессу.

Каждую угрозу T_{ij} из множества угроз перекрывает соответствующее множество сервисов безопасности:

$$\forall_{(T_{ij})} \in_T \exists_{(\{C_{ij1}C_{ij2},\dots,C_{ijn}\})} \in_C,$$

где n – количество сервисов безопасности, противодействующих угрозе T_{ij}.

Это условие означает, что каждой угрозе T_{ij} из множества угроз T соответствует подмножество сервисов безопасности $\{C_{ij1}, C_{ij2}, \dots, C_{ijn}\}$ множества сервисов C.

5. Реализация модели системы защиты ИТ

На основе предложенной модели разработана автоматизированная система разработки профиля защиты и задания по безопасности. Были созданы 12 таблиц справочных баз данных: «Объекты защиты», «Угрозы», «Сервисы безопасности», «Предложения безопасности», «Требования безопасности», «Правила политики безопасности», «Параметры правил политики безопасности», «Типовые прикладные решения на основе сервисов безопасности», «Правила политики безопасности, реализуемые типовыми прикладными решениями на основе сервисов безопасности», «Параметры сервисов безопасности типовых прикладных решений», «Оценочные уровни доверия», «Требования доверия».

Работа автоматизированной системы основана на использовании графического последовательного интерфейса, работа с которым заключается в определении состава структурных объектов ИТ.

После подключения справочной базы данных пользователь определяет состав структурных объектов ИТ, воспользовавшись элементом управления типа «флажок», расположенным в верхней части окна «Система поддержки принятия решения». Установка или снятие «флажка», соответствующего какому-либо объекту защиты ИТ, запускает механизм выполнения SQL-запроса к справочной базе данных. В запросе принимают участие таблицы базы данных, содержащие информацию об объектах защиты ИТ, угрозах, сервисах безопасности и правилах политики безопасности организации. Запрос осуществляет выборку объектов защиты ИТ и проверку, установлен ли для данного объекта «флажок» включения его в профиль защиты.

Использование автоматизации разработки профиля защиты задания по безопасности защищенных ИТ с применением типовых решений позволяет наглядно и эффективно представлять и манипулировать большими объемами данных, необходимыми для выполнения этапов разработки защищенных ИТ (рис. 5–8). Этапы разработки представляются в удобной графической форме. Такая общая визуализация процессов обеспечения защищенности ИТ позволяет оперативно генерировать различные варианты защиты, сравнивать их между собой с точки зрения эффективности и в результате выбирать оптимальный вариант построения или модификации системы защиты ИТ.

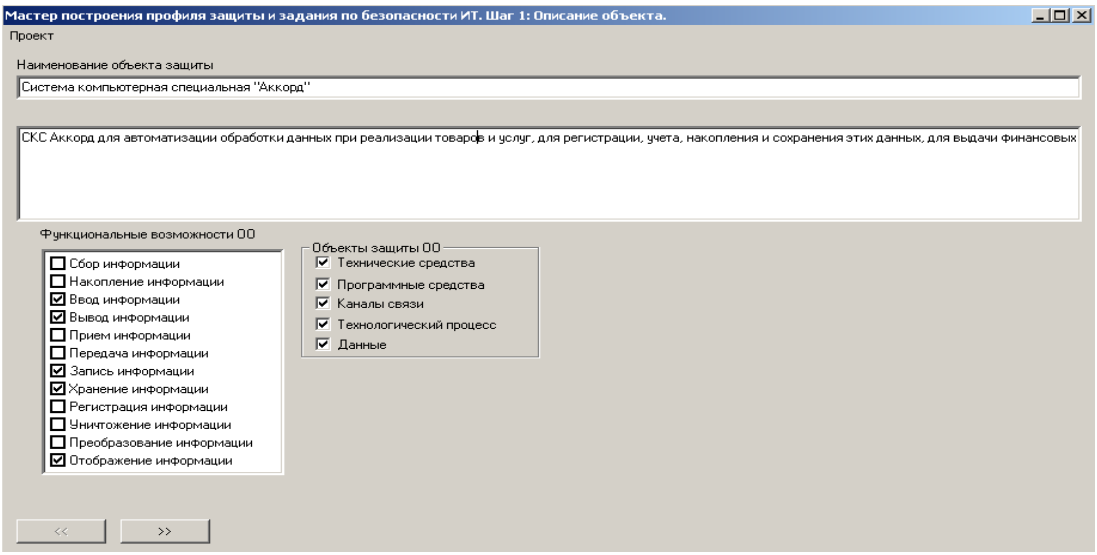

Рис. 5. Определение функциональных возможностей и состава объекта

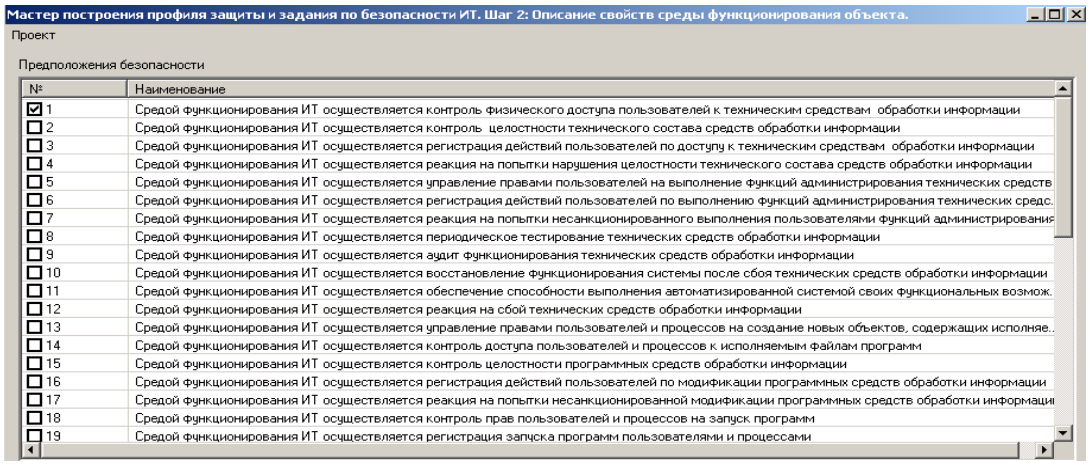

Рис. 6. Описание свойств среды функционирования объекта

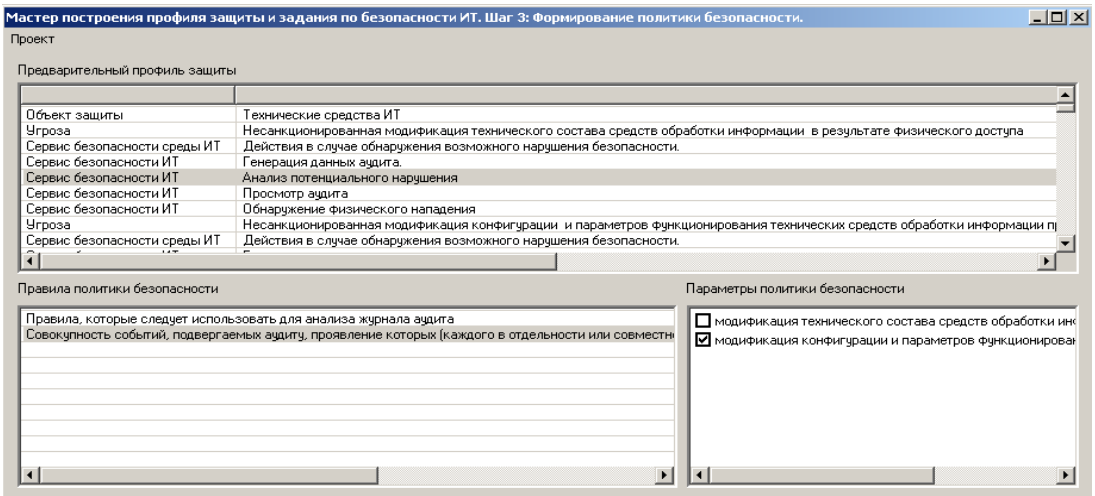

Рис. 7. Формирование политики безопасности

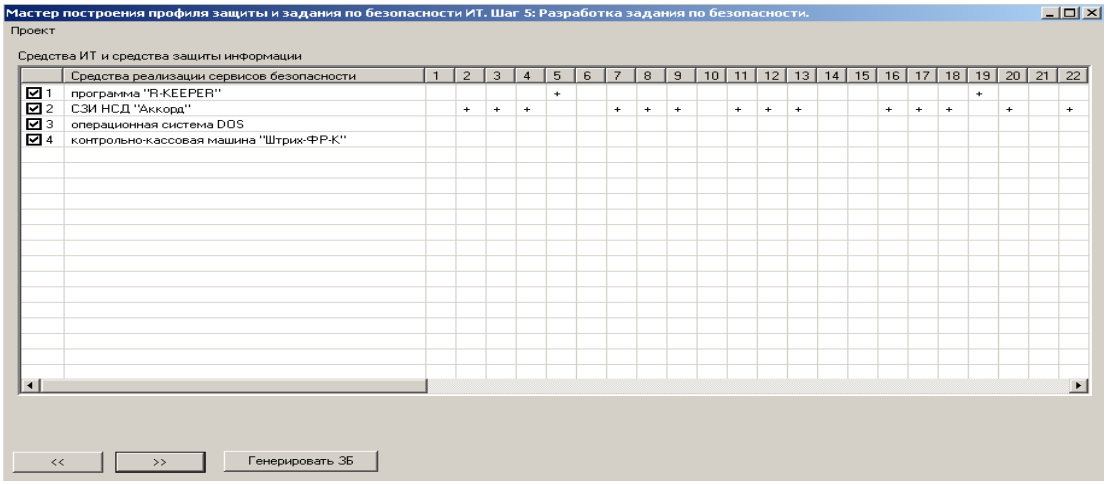

Рис. 8. Разработка задания по безопасности

Заключение

Предлагаемая модель обеспечивает полное перекрытие угроз: каждому классу объектов соответствует весь перечень возможных угроз как для всего класса объектов, так и для каждого объекта в классе.

Так как каждой угрозе поставлен в соответствие перечень сервисов безопасности, обеспечивающих полное перекрытие конкретной угрозы, все множество сервисов безопасности обеспечивает полное перекрытие множества всех угроз.

Каждому типовому сервису безопасности сопоставлены множества требований безопасности. Эти множества разработаны на основе каталога требований безопасности, содержащегося в СТБ 34.101.-2004 (ИСО/МЭК 15408:1999) [12].

Из подхода к моделированию системы безопасности ИТ как совокупности типовых сервисов безопасности следует, что сервисный подход целесообразно применить и к описанию прикладных решений в области защиты информации. Средство ИТ или средство защиты, реализующее типовой сервис безопасности, в таком случае можно рассматривать как типовое. Для оценки способности средств ИТ или средств защиты информации реализовывать сервисы безопасности каждому сервису безопасности сопоставлены множества требований безопасности, разработанные на основании каталога функциональных требований безопасности [12].

Список литературы

1. Липаев В.В. Программно-технологическая безопасность информационных систем / В.В. Липаев. – М. : МИФИ, 1997. – 143 с.

2. Обеспечение информационной безопасности в сфере экономики / О.В. Голосов [и др.] // Информационная безопасность : учебное пособие для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности. – М. : МГФ «Знание», 2005. – С. 255–298.

3. Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению : ГОСТ 19.503–79. – Введ. 01.01.80. – М. : ИПК Издательство стандартов, 1998. – С. 79–81.

4. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство : ГОСТ Р 51188–98. – Введ. 01.07.99. – М. : ИПК Издательство стандартов, 1998.

5. Защита информации. Объект информатизации. Факторы, воздействующие на информацию : ГОСТ Р 51275–99. – Введ. 12.05.99. – М. : ИПК Издательство стандартов, 1999.

6. Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению : ГОСТ 19.504–79. – Введ. 01.01.80. – М. : ИПК Издательство стандартов, 1998. – С. 81–83.

7. Единая система конструкторской документации. Эксплуатационные документы : ГОСТ 2.601–95. – Введ. 01.07.96. – М. : ИПК Издательство стандартов, 1995.

8. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения : ГОСТ 34.003-90. – Введ. 01.01.92. – М. : ИПК Издательство стандартов, 1990.

9. Информационная технология. Виды испытаний автоматизированных систем : ГОСТ 34.603–92. – Введ. 01.01.93. – М. : ИПК Издательство стандартов, 1992.

10. Конявский, В. А. Компьютерная преступность : в 2 т. / В.А. Конявский, С.В. Лопаткин. – М. : РФК-Имидж Лаб, 2006. – Т.1. – 560 с.

11. Конявский, В.А. Основы технологической защиты электронных документов / В.А. Конявский // Компьютерная преступность и информационная безопасность ; под общ. ред. А.П. Леонова. – Минск : АРИЛ, 2000. – С. 298–350.

12. Критерии оценки безопасности информационных технологий : СТБ 34.101-2004 (ИСО/МЭК 15408:1999) – Введ. 21.07.2004. – Минск : Госстандарт, 2004.

Поступила 02.08.12

ООО «МАРФИ»,
Минск, Переходная, 64-6
e-mail: 001@marfi.by

H.V. Fralou

A SYSTEM APPROACH TO INFORMATION TECHNOLOGY PROTECTION

The suggested model of information security system works using security services. The model is chosen based on the following criteria of systems quality: suitability criterion, optimality criterion and criterion of superiority based on the proposed classification of security threats. The proposed model is a set of security services that can be realized in the IT environment or in the IT itself with the help of information security facilities.