УДК 004.056

И. В. Бондарь

МЕТОДИКА ПОСТРОЕНИЯ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ*

Рассматривается методика построения модели угроз безопасности информации. Целью моделирования является контроль уровня защищенности информационной системы методами анализа риска и разработка эффективной системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз соответствующими защитными мерами.

Ключевые слова: модель угроз, информационная система, модель системы защиты информации.

В настоящее время особую актуальность приобретает разработка методологии, позволяющей в рамках единого подхода решать задачи проектирования автоматизированных систем в защищенном исполнении с соблюдением требований нормативно-методических документов и автоматической генерацией перечня защитных мер и поиска оптимального набора средств защиты информации (СЗИ), соответствующих данному перечню.

Одними из основных задач обеспечения информационной безопасности являются определение перечня угроз и оценка рисков воздействия актуальных угроз, что позволяет обосновать рациональный состав системы защиты информации. Хотя задачи такого рода уже решаются (см., например, [1; 2]), в том числе и в рамках единой методологии [3; 4], все они не лишены ограничений и направлены на формирование модели угроз, пригодной для решения частной задачи. Особо хочется отметить редкость попыток визуализации моделей угроз.

В данной статье представлена методика моделирования угроз безопасности информации для автоматизированных систем, основанная на геометрической модели [5]. Эта методика интересна прежде всего универсальностью учета негативных воздействий, что ранее встречалось лишь в работе [1], где модель строилась на основе теории возмущений, и возможностью визуализации результата [6–8]. Обычный путь визуализации – использование карт Кохонена с присущими им ограничениями и недостатками – автором не рассматривается, что повышает универсальность решения.

Геометрическая модель СЗИ. Пусть $P = (p_1, p_2, \ldots, p_z)$ – множество средств защиты, а $A = (a_1, a_2, \ldots, a_n)$ – множество атак. Те атаки, которые не могут быть выражены комбинациями атак, назовем независимыми. Их множество A' является подмножеством множества A – базисом атак. Выберем для построения геометрической модели СЗИ пространство R^n, размерность которого совпадает с мощностью множества A.

Любой атаке $A_i \in A$ поставлены в соответствие определенные средства защиты $(p'_1, p'_2, \ldots, p'_k) \subseteq P$. Обозначим это множество $\{p'_1, p'_2, \ldots, p'_l\} = P_{ri}$.

Если средство P_j не принадлежит множеству P_{ri}, то для него атака A_i не опасна.

Оси координат в пространстве R^n представляют собой классы угроз. Единица измерения на осях координат является независимой атакой, которой поставлено в соответствие средство защиты. Для каждой атаки значения координат соответствующего вектора указывают на средства защиты, входящие в состав исследуемой системы.

В качестве примера, рассмотрим атаку «НСД к информации, хранящейся на АРМ, внешним нарушителем» в декартовом пространстве, где ось x – угрозы, связанные с физической охраной; y – угрозы, связанные с программно-аппаратной защитой; z – угрозы, связанные с организационно-правовой защитой (рис. 1). Атака может быть реализована в случае невыполнения трех мер защиты: «Посторонний в контролируемой зоне», «Незаблокированный сеанс ОС» и «Нарушение ПБ».

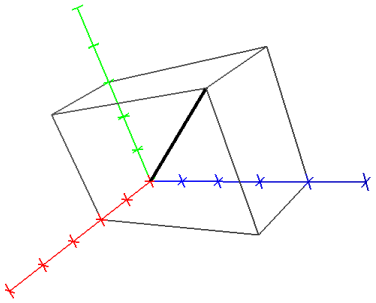

Рис. 1. Модель атаки «НСД к информации, хранящейся на АРМ, внешним нарушителем»

Данная атака может быть реализована и другими способами, такими как «Подключение к техническим средствам и системам ОИ», «Использование закладочных средств», «Маскировка под зарегистрированного пользователя», «Дефекты и уязвимости ПО», «Внесение программных закладок», «Применение вирусов и другого вредоносного программного кода», «Хищение носителя защищаемой информации», «Нарушение функционирования ТС обработки информации» (рис. 2).

*Работа выполнена в рамках реализации ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы» (ГК № 07.514.11.4047 от 06.10.2011).

Первоначально каждый вектор P_i находится в первом координатном октанте. Построим в R^n поверхность выпуклого многогранника S так, чтобы каждая из его вершин совпадала с концом одного из векторов $p_1, p_2, \ldots, p_z$. Поверхность многогранника S вместе с векторами $p_1, p_2, \ldots, p_z$ будем рассматривать в качестве геометрической модели СЗИ.

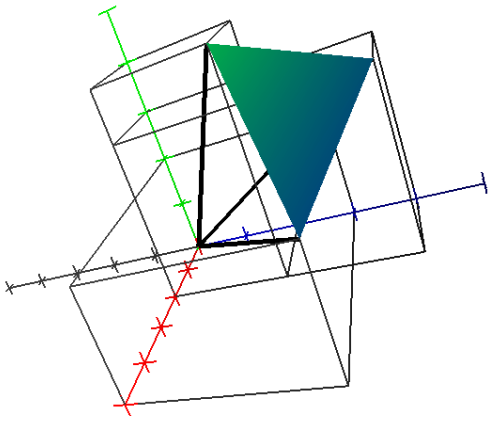

Рис. 2. Модель атаки «НСД к информации, хранящейся на АРМ, внешним нарушителем»

Результат воздействия любой атаки A_i естественно формализовать отражением вектора вдоль оси с невыполненной мерой защиты. Благодаря такому способу моделирования векторы, соответствующие средствам, для которых данная атака не опасна, не изменят своего положения (рис. 3).

Итак, после воздействия атаки A_j при предложенном способе моделирования изменится лишь i-я координата векторов $p_1, p_2, \ldots, p_z$, входящих в геометрическую модель, а все остальные координаты останутся без изменения.

По результатам моделирования атак можно судить о чувствительности или нечувствительности информационной системы (ИС) к возмущающим воздействиям. Если координаты многогранника принадлежат первому координатному октанту, то делается вывод о нечувствительности ИС к возмущающему воздействию, в противном случае делается вывод о недостаточности защитных мер. Мера устойчивости сводится к проведению такого количества итераций, при котором ИС остается невозмущенной к воздействиям комбинаций атак.

Модель угроз. Первичный перечень угроз формируется комбинациями всевозможных факторов, воздействующих на защищаемую информацию, категориями средств защиты и уровнями воздействия нарушителей (рис. 4).

Выявление и учет факторов, которые воздействуют или могут воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, обеспечивающих защиту информации на объекте информатизации. Полнота и достоверность выявления факторов достигается путем рассмотрения полного множества факторов, воздействующих на все элементы объекта информатизации на всех этапах обработки информации. Перечень основных подклассов (групп, подгрупп и т. д.) факторов в соответствии с их классификацией представлен в разделе 6 ГОСТ 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Угрозы утечки информации по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, т. е. определяются характеристиками технического канала утечки информации.

Формирование вторичного перечня угроз происходит за счет его пополнения на основе статистики об имевших место инцидентах и исходя из условной степени их деструктивного воздействия.

Степень возмущающего воздействия может быть определена:

– вероятностью возникновения угрозы;

– потерей от реализации угрозы;

– временем восстановления системы.

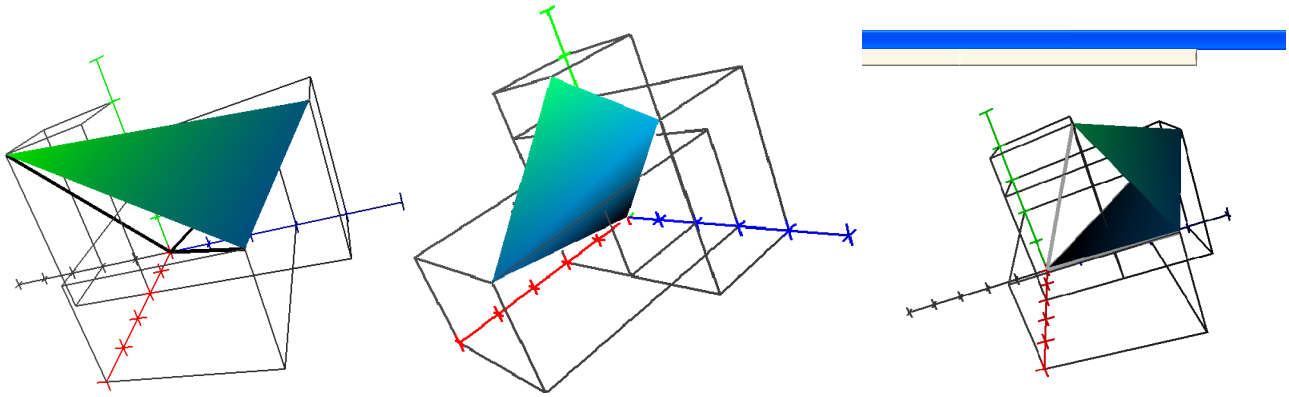

Рис. 3. Результаты моделирования

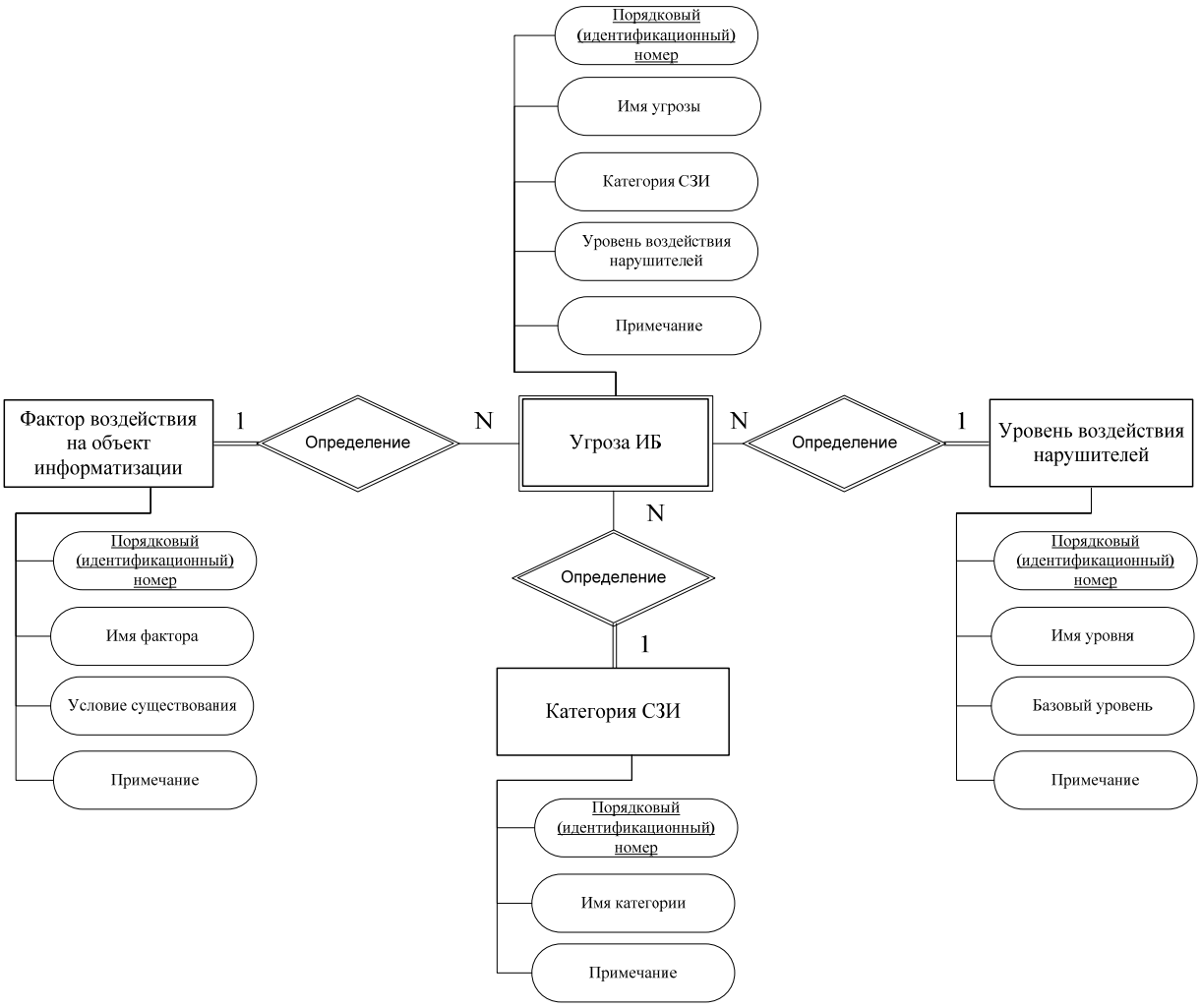

Рис. 4. ER-модель базы данных модели угроз в нотации Чена

Возмущающее воздействие может привести:

– к нарушению конфиденциальности информации (копированию или несанкционированному распространению), когда при реализации угроз не осуществляется непосредственного воздействия на содержание информации;

– несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение информации или ее уничтожение;

– несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИС, в результате которого происходит блокирование информации;

– потере подотчетности пользователей системы или субъектов, действующих от имени пользователя, что особенно опасно для распределенных систем;

– потере аутентичности данных;

– потере достоверности систем.

Мера риска, позволяющая сравнить угрозы и выстраивать их по приоритетности, может быть определена общим ущербом от каждого вида проблем.

Результатом оценки риска возникновения каждой угрозы должно явиться:

– комплексное применение соответствующих средств защиты информации;

– разумное и целевое принятие рисков, обеспечивающее полное удовлетворение требований политик организации и ее критериев принятия рисков;

– максимально возможный отказ от рисков, перенос связанных бизнес-рисков на другие стороны, например на страховщиков, поставщиков и пр.

Рассматриваемая методика построения модели угроз позволяет решать задачи разработки частных моделей угроз безопасности информации в конкретных системах с учетом их назначения, условий и особенностей функционирования. Целью такого моделирования является контроль за уровнем защищенности ИС методами анализа риска и разработка эффективной системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз.

В дальнейшем данная методика может явиться основой для разработки универсальных алгоритмических, а затем и математических моделей безопасности, эффективно сочетающих в себе требования нормативно-методических документов, методологию построения моделей угроз, моделей нарушителя и т. д. Наличие подобного методологического обеспечения

позволит перейти на качественно более высокий уровень проектирования, разработки и оценки защищенности систем защиты информации.

Библиографические ссылки

1. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности : монография. Киев : Изд-во Гос. ун-та информ.-коммуникац. технологий, 2009.

2. Васильев В. И., Машкина И. В., Степанова Е. С. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушений информационной безопасности // Изв. Юж. федер. ун-та. Технические науки. 2010. Т. 112, № 11. С. 31–40.

3. Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave) Framework : Techn. Rep. CMU/SEI-SS-TR-017 / C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson ; Carnegie Mellon Univ. Pittsburgh, PA, 2005.

4. Burns S. F. Threat Modeling: a Process to Ensure Application Security // GIAC Security Essentials Certification Practical Assignment. Version 1.4c / SANS Inst. Bethesola, Md, 2005.

5. Попов А. М., Золотарев В. В., Бондарь И. В. Методика оценки защищенности информационной системы по требованиям стандартов информационной безопасности // Информатика и системы упр. / Тихоокеан. гос. ун-т. Хабаровск, 2010. № 4 (26). С. 3–12.

6. Анализ надежности и риска специальных систем : монография / М. Н. Жукова, В. В. Золотарев, И. А. Панфилов и др. ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2011.

7. Жуков В. Г., Жукова М. Н., Стефаров А. П. Модель нарушителя прав доступа в автоматизированной системе // Програм. продукты и системы / НИИ Центрпрограммсистем. Тверь, 2012. Вып. 2. С. 72–75.

8. Система поддержки принятия решений по защите информации «ОАЗИС» / И. В. Бондарь, В. В. Золотарев, А. В. Гуменникова, А. М. Попов // Програм. продукты и системы / НИИ Центрпрограммсистем. Тверь, 2011. Вып. 3. С. 186–189.

I. V. Bondar

CONSTRUCTION METHOD FOR INFORMATION SECURITY THREAT MODELS OF AUTOMATED SYSTEMS

The authors consider a technique of threat models constructing. The purpose of modeling is to control the information system security level with risk analysis methods and describe the development of an effective information security system that ensures the neutralization of the supposed threats with appropriate security measures.

Keywords: threat model, information system, information security system model.

УДК 004.932

В. В. Буряченко

СТАБИЛИЗАЦИЯ ВИДЕО ДЛЯ СТАТИЧНОЙ СЦЕНЫ НА БАЗЕ МОДИФИЦИРОВАННОГО МЕТОДА СООТВЕТСТВИЯ БЛОКОВ

Рассмотрены основные подходы к стабилизации видеоматериалов, в частности нахождение глобального движения кадра, вызванного внешними воздействиями. Построен алгоритм стабилизации видеоматериалов на основе модифицированного метода соответствия блоков для последовательных кадров.

Ключевые слова: *стабилизация видео, метод соответствия блоков, гауссово распределение.*

Цифровая система стабилизации изображения в первую очередь оценивает нежелательные движения, а затем исправляет последовательности изображений, компенсируя влияние внешних факторов: нестабильности съемки, погодных условий и т. д. Вполне вероятно, что аппаратные системы захвата движения будут включать в себя стабилизацию изображения, поэтому данное исследование сосредоточено на моделировании и реализации алгоритмов, которые могут эффективно работать на аппаратных платформах.

Существует два основных подхода к решению проблемы стабилизации видеоматериалов: механический подход (оптическая стабилизация) и цифровая обработка изображений. Механический подход применяется в оптических системах для настройки датчиков движения во время дрожания видеокамеры и означает использование устойчивой установки видеокамеры или наличие гироскопических стабилизаторов. Несмотря на то что этот подход может хорошо работать на практике, он почти не используется из-за высокой стоимости приборов стабилизации и наличия