УДК 681.3.06:519.248.681

Л. В. СКРЫПНИК, д-р. техн. наук, А. В. ПОТИЙ, канд. техн. наук.

ГИБКОСТЬ И СПЕЦИАЛИЗАЦИЯ ПРОФИЛЯ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Введение

На сегодняшний день в Украине окончательно сформировалась точка зрения, заключающаяся в том, что обеспечение безопасности информации при её обработке в автоматизированных системах (АС) осуществляется на всех стадиях жизненного цикла АС, на всех технологических этапах обработки информации и во всех режимах функционирования АС путем создания и внедрения в АС комплексной системы защиты информации (СЗИ) как составной и неотъемлемой части АС [1]. Анализ действующей нормативной базы, как отечественной, так и международной, показал, что наряду с задачей разработки системы защиты информации, интегрированной в АС, актуальной является задача оценки защищенности информации в АС. Причем последняя задача должна решаться как для уже существующих, так и для проектируемых СЗИ. Доминирующим подходом при решении этой задачи на сегодняшний день является метод, основанный на разработке профиля защиты АС с последующей его оценкой. *Профиль защиты* представляет собой реализационно-независимую совокупность требований безопасности информационных технологий (ИТ-безопасности), которые включают в себя: 1) функциональные требования безопасности, определяющие набор функций безопасности, направленных на решение задач защиты и обеспечения требуемого уровня защиты и 2) требования адекватности, обеспечивающие высокую степень уверенности в правильности выбора и надежности функционирования механизмов безопасности. (Здесь и далее используется терминология международного стандарта ISO/IEC 15408 [5]. Причем термины «автоматизированная система» [1, 3, 4], «компьютерная система» [2] являются синонимами термина «объект оценки (TOE)» [5]. Все эти объекты являются системами информационных технологий (ИТ-системы).)

При анализе и оценке профиля защиты эксперт устанавливает, насколько рассматриваемый профиль отвечает предъявленным к нему требованиям функциональной полноты, непротиворечивости, реализуемости, адекватности. По нашему мнению, помимо этих требований к профилю защиты необходимо предъявить новое требование – гибкость. Обоснование необходимости введения данного требования и является целью данной статьи.

1. Требования к профилю защиты

К профилю защиты предъявляют следующие требования.

1. *Функциональная полнота.* Профиль защиты должен содержать функционально полный набор функций безопасности, что обеспечивает решение всех задач защиты и предотвращение выявленных угроз безопасности.
2. *Непротиворечивость (согласованность).* Функция безопасности характеризует проявление свойств системы защиты информации в данной совокупности соотношений и представляет собой способ действия системы при взаимодействии элементов системы между собой, а также при взаимодействии системы с внешней средой (средой эксплуатации). В связи с этим требование непротиворечивости направлено на учет взаимозависимости функциональных требований между собой и согласованности функциональных требований и требований адекватности. Последнее означает учет влияния внешних факторов на профиль защиты. В общем, соблюдение требования непротиворечивости направлено не обеспечение целостности СЗИ как системы.
3. *Реализуемость* (техническая реализуемость). Требование отражает техническую возможность реализации определенного согласованного набора функций безопасности, с учетом имеющихся ограничений на ресурсы, выделяемых на реализацию системы.
4. *Адекватность.* Наиболее ёмкое требование, направленное на обеспечение требуемого уровня безопасности информации, т.е. адекватности СЗИ угрозам безопасности информации, существующим в конкретной среде эксплуатации и в конкретной ИТ-системе. Адекватность требует осуществления оценки эффективности функций безопасности и оценки корректности реализации функций безопасности.

Поскольку профиль защиты, по сути, представляет собой функциональную модель СЗИ, то перечисленные требования профиля преобразуются в свойства системы, которые будут характеризовать эффективность функционирования СЗИ. Однако, перечисленные требования направлены на обеспечение статических свойств СЗИ, в то время как процесс защиты информации является непрерывным

динамическим процессом. Как антропогенная система, СЗИ в числе многих свойств, таких как целенаправленность, целостность, управляемость и других, должна обладать свойством непрерывности развития. Игнорирования концепции развития в процессах проектирования, производства и эксплуатации систем приводит к созданию нежизнеспособных систем. Обеспечение свойства непрерывности требует учета динамической природы функционирования СЗИ, совершенствования, как технологий защиты информации, так и технологий, методов и способов осуществления несанкционированного доступа к защищаемой информации. В зависимости от складывающейся обстановки, с точки зрения состава и возможностей реализации тех или иных угроз безопасности, может изменяться состав решаемых системой задач защиты. Причем это изменение носит не только количественный характер (появление новых задач защиты, отпадение необходимости решения существующих задач защиты), но и качественный характер (изменение степени риска той или иной угрозы приводит к изменению приоритетности задачи защиты и, как следствие, к изменению уровня адекватности профиля защиты). С этой точки зрения непрерывность защиты информации заключается в постоянном анализе среды эксплуатации АС, оперативном анализе (оценке) рисков и выработке управляющих воздействий, направленных на коррекцию задач защиты. Изменение внешних условий влечет за собой изменение способа действия системы при её взаимодействии с внешней средой, то есть приводит к изменению функций безопасности. В более широком смысле это приводит к изменению профиля защиты и, в конечном счете, к необходимости изменения состава средств и механизмов защиты или, как минимум, к изменению режимов их работы. Таким образом, функциональная структура СЗИ не является статичной, раз и навсегда разработанной. Профиль защиты в процессе функционирования системы будет изменяться, модифицироваться. Из выше сказанного следует, что при разработке профиля защиты к нему необходимо предъявлять еще одно требование – требование *гибкости*. Причиной, объективно побуждающей введение такого требования, является усиливающееся, особенно в современных АС и СЗИ, противоречие между необходимостью решения быстроизменяющихся задач защиты и сложностью обеспечения при этом высокой эффективности СЗИ с помощью существующих средств защиты. Ясно, что высокую гибкость системы и её высокую эффективность в любых условиях изменяющейся обстановки обеспечить достаточно сложно и дорого. С одной стороны, наибольшая эффективность защиты может быть достигнута лишь при решении относительно узкого класса задач защиты путем создания «жесткой», узкопрофильной, специализированной СЗИ. Однако, при работе СЗИ в условиях неопределенности относительно состояния среды эксплуатации, быстроизменяющегося состава и качества задач защиты наибольшей эффективностью будут обладать широкопрофильные, гибкие СЗИ, с большим набором функций безопасности. Возникает ***проблема нахождения оптимального состояния гибкости и эффективности системы защиты информации.***

2. Гибкость как экономическая категория

Гибкость системы это свойство системы, состоящее в возможности её совершенствования, расширения и придания ей новых качеств [6]. Гибкость предполагает легкое, то есть без особых усилий и затрат, и достаточно быстрое изменение того или иного состояния системы. Применительно к СЗИ можно сформулировать следующее определение. ***Гибкая система защиты информации это совокупность в разных сочетаниях механизмов безопасности, средств защиты информации, программного и аппаратного обеспечения, системы анализа (оценки) рисков и системы управления, обеспечивающих функционирование СЗИ в автоматизированном режиме, обладающая свойством автоматизированной перестройки при решении задач защиты различного состава в пределах своих технических характеристик.***

Интенсивное изменение среды эксплуатации приводит к тому, что система защиты вынуждена приспосабливаться (адаптироваться) к решению новых задач защиты, обладающих определенной степенью разнообразия. Однако не всякая способность адаптации системы к быстрой смене задач защиты, быстрой смене и модификации функциональных требований может квалифицироваться как гибкость. Адаптация, достигаемая «любой ценой» с точки зрения затрачиваемых ресурсов, не может признаваться гибкостью. Отсюда, *гибкость как экономическая категория отражает способность СЗИ к эффективной адаптации, то есть рассматривается, как способность системы изменять свои цели функционирования без существенных затрат.*

Изменение целей функционирования жестких систем связано, как правило, либо с техническим перевооружением, либо с реконструкцией СЗИ. Тогда как гибкие системы могут длительно и эффективно удовлетворять постоянно изменяющиеся потребности собственника защищаемых ресурсов без технического перевооружения и модификации системы ЗИ.

Каким образом охарактеризовать гибкость профиля АС и, следовательно, гибкость СЗИ? По аналогии с решением подобной задачи для производственных систем [7] введем показатель

$$G(t_к, t_н) = J_{из}(t_к, t_н)/J_з(t_к, t_н),$$

где $G(t_к, t_н)$ – гибкость профиля защиты в период $(t_к, t_н)$; $J_{из}(t_к, t_н)$ – индекс, характеризующий изменение степени разнообразия задач защиты в системе в период $(t_к, t_н)$; $J_з(t_к, t_н)$ – индекс, характеризующий изменение приведенных динамических затрат, связанных с функционированием системы в период $(t_к, t_н)$.

Чем больше значение G, тем система более гибкая.

Значение G зависит от величины интервала $(t_к, t_н)$. Прежде чем изложить возможный подход к оценке этого интервала рассмотрим понятия техническое перевооружение и реконструкция относительно системы ЗИ. *Техническим перевооружением* будем называть комплекс мероприятий по повышению до современного уровня технического (программного, аппаратного, алгоритмического, математического) уровня элементов и подсистем СЗИ путем внедрения новых технологий обработки информации, программного и аппаратного обеспечения и других мер, направленных на обеспечение и повышение адаптивности функционирования СЗИ. Техническое перевооружение обусловлено развитием методов несанкционированного доступа к защищаемой информации, изменением возможностей злоумышленника по осуществлению атак, качественным изменением защищаемых ресурсов и другими условиями. *Реконструкция* системы ЗИ предполагает полную перестройку системы ЗИ по новым принципам. Необходимость реконструкции чаще всего вызывается физическим и моральным старением СЗИ.

Чем продолжительнее период между двумя последовательными техническими перевооружениями или реконструкциями, тем большей гибкостью при условии стабильной эффективности функционирования обладает СЗИ. С другой стороны, чем продолжительнее этот период, тем возможен больший потенциальный ущерб от нарастающего физического износа и морального старения механизмов и средств защиты информации. Особенно это зависит от продолжительности межреконструкционного периода. Это противоречие порождает необходимость решения следующих задач:

– нахождение оптимальной продолжительности межреконструкционного периода;

– выбор рациональных сроков начала и окончания работ по подготовке и проведению перевооружения и реконструкции СЗИ.

Решение этих задач направлено на предотвращение экономического ущерба, вызываемого использованием изношенных (устаревших) и преждевременной ликвидации недоамортизированных элементов СЗИ, а также «замораживанием» различного рода ресурсов. На основе решения этих задач оптимизации могут быть найдены значения периода $(t_к, t_н)$, для которого определяются значения $G(t_к, t_н)$. Полученные значения $G(t_к, t_н)$ могут рассматриваться как количественные характеристики оптимальной гибкости СЗИ.

Показатель G также зависит от индекса изменения степени разнообразия задач защиты. Среди факторов, оказывающих влияние на разнообразие задач защиты можно выделить следующие:

– степень вариативности целей функционирования АС (надсистемы), интегрированной частью которой является СЗИ. АС и СЗИ по своей сути являются многоцелевыми системами. В таких системах цели либо задаются с вышестоящих уровней иерархии, либо определяется из сложившейся ситуации лицом, принимающим решение;

– вариативность среды эксплуатации. Изменчивость среды эксплуатации складывается из возможности изменения ресурсов злоумышленника, что в свою очередь приводит к изменению количественного и качественного состава угроз безопасности, изменения защищаемых ресурсов, совокупность которых определяется изменчивостью потребностей собственника ресурсов.

Если степень изменения задач защиты, как потребностей собственника защищаемых ресурсов, позволяет в течение длительного периода эффективно использовать для их решения жесткую систему, то оптимальной будет невысокая степень гибкости. Это характерно для однообъектных систем обработки информации, решающих узкий класс задач защиты. Для распределенных АС характерно быстрое изменение внешних условий, постоянная модификация задач защиты, что приводит к изменению представлений об оптимальной гибкости. Если жесткая система начинает входить в противо-

речие с необходимостью быстрого и эффективного изменения функционального состава системы, оптимальной становится более гибкая система.

Таким образом, существуют области эффективного функционирования СЗИ различной степени гибкости. Поэтому стремление в разных условиях создавать СЗИ на основе одинаковых по степени гибкости профилей защиты экономически нецелесообразно.

3. Специализация профиля защиты

В вопросе гибкости СЗИ необходимо обратить внимание на такой аспект как специализация системы. *Специализация* – это концентрация, сосредоточение деятельности на решение какой-либо задачи, на выполнение какой-либо операции или функции. Не возникает сомнений, что в зависимости от совокупности решаемых задач защиты системы ЗИ будут иметь различную степень специализации. Различные степени специализации создают различные условия для гибкости профиля защиты.

Имеющиеся на сегодняшний день нормативные документы по оценки защищенности информационных технологий, как международные [5], так и национальные [1-4] позволяют сформулировать следующий взгляд на специализацию СЗИ.

Специализация СЗИ зависит от типа задач защиты, на решение которых направлены функции безопасности. Тип задач определяется в зависимости от класса угроз безопасности, на предотвращение которых направлено функционирование СЗИ. Согласно нормативным документам, профиль защиты должен содержать функциональные требования (ФТ), которые определяют набор функций безопасности СЗИ. Причем множество функциональных требований декомпозируются на классы по целевому признаку. Так, в международном стандарте ISO/IEC 15408 определено тринадцать классов функциональных требований, в отечественном нормативном документе НД ТЗИ 2.5.–004–99 – пять классов. Анализ содержания функциональных требований (то есть, семейств и компонент) позволят разбить их на три основные категории.

1. Категория специальных функциональных требований, в которую входят классы ФТ, целевой направленностью которых является решение задач защиты по непосредственному предотвращению конкретных типов угроз безопасности. В самом общем случае в данную категорию можно отнести классы ФТ, предотвращающие угрозы конфиденциальности, целостности и доступности информации.

2. Категория общих функциональных требований объединяет классы ФТ, целевой направленностью которых является решение общих задач, не зависящих от конкретного типа или набора предотвращаемых системой угроз безопасности. К этой категории можно отнести классы ФТ, направленные на решение задач управления системой защиты информации, аудита безопасности, адекватности (гарантированности) защиты и т.д. Отметим, что данные ФТ практически всегда включаются в систему защиты информации.

3. Категория вспомогательных функциональных требований. В данную категорию входят ФТ, целевой направленность которых является решение задач по обеспечению работы, расширению и усилению функциональных возможностей механизмов безопасности, которые реализуют функции безопасности, определяемые специальными требованиями.

Целевую специализацию будет определять совокупность специальных функциональных требований. Поскольку в настоящее время преобладают взгляды построения комплексных систем защиты информации с непрерывным процессом обеспечения безопасности данных, то современные СЗИ будут обладать специализацией по нескольким классам специальных ФТ, с выделением приоритетности отдельного класса функциональных требований в зависимости от целевого предназначения АС (например, в системах электронных платежей предъявляются усиленные требования к обеспечению целостности данных, в военных системах управления и связи – к конфиденциальности, в системах хранения данных – к доступности). Приоритетность того или иного класса ФТ может быть определена через количество функциональных компонент, включаемых в профиль защиты из конкретного класса ФТ. Специализация по классам ФТ будет отличаться разнообразием решаемых задач защиты, что создает благоприятные предпосылки для эффективного использования сложных , комплексных и, в конечном итоге, гибких СЗИ.

В заключение сформулируем главную цель СЗИ, которая позволяет определить критерий предпочтительности параметров профиля защиты. Такой целью можно считать **эффективное (т.е. своевременное, оперативное, адекватное) решение заданной совокупности задач защиты (в плане удовлетворения потребностей собственника защищаемых ресурсов) при ограничениях, накладываемых на используемые ресурсы, возрастании потенциальных возможностей злоумышлен-**

ника по несанкционированному доступу и использованию защищаемых ресурсов и одновременном совершенствовании среды эксплуатации и не ухудшении свойств и характеристик АС (надсистемы).

Заключение

1. Профиль защиты АС должен отражать не только статические свойства СЗИ, но и ее динамические свойства, отражать свойство развития системы и непрерывности процесса защиты информации. В связи с этим помимо известных требований функциональной полноты, непротиворечивости, реализуемости, адекватности, к профилю защиты автоматизированной системы необходимо предъявлять требование гибкости.

2. Гибкость, как экономическая категория, отражает способность СЗИ к эффективной адаптации, то есть рассматривается как способность системы изменять свои цели функционирования без существенных затрат. Требования гибкости позволит учитывать вариативность задач защиты, изменчивость среды эксплуатации, которая характерна для современных автоматизированных систем. В зависимости от степени варитативности задач защиты создаются системы с различной степенью гибкости, что позволяет сделать вывод о существовании различных областей эффективного функционирования гибких СЗИ.

3. Функциональные требования могут быть разбиты на три основных категории: специальные, общие и вспомогательные. В современных автоматизированных системах профили защиты будут специализироваться по нескольким классам специальных требований, что создает условия разработки гибкой системы защиты с «широким» профилем.

Список литературы. 1. *Общие положения по защите информации в компьютерных системах от несанкционированного доступа.* НД ТЗИ 1.1.–002–99. ДСТСЗИ СБ Украины. Киев, 1999. **2.** *Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа.* НД ТЗИ 2.5.–004–99.–ДСТСЗИ СБ Украины. Киев, 1999. **3.** *Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа.* НД ТЗИ 2.5.–005–99. ДСТСЗИ СБ Украины. Киев, 1999. **4.** *Средства вычислительной техники.* Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992. **5.** *ISO/IEC 15408.* Information technology – Security techniques – Evaluation criteria for IT security. **6.** *Першиков В.И., Савинков В.М.* Толковый словарь по информатике. М.: Финансы и статистика, 1991. **7.** *Системное проектирование радиоэлектронных предприятий с гибкой автоматизированной технологией* / Под ред. В.А. Мясникова, Ф.И. Темникова. М.: Радио и связь, 1990.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 30.03.2001