1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ

УДК 681.3.06

МЕТОДИКА ФОРМИРОВАНИЯ ПРОФИЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Леонид Осинский, Андрей Чернышев*
Министерство Обороны Украины
**Служба безопасности Украины*

Анотація: **Пропонується методика формування профилю захищеності інформаційних технологій на підставі теорії нечітких множин.**
Summary: **The technique of formation of a protection profile of information technologies is offered on the basis of the theory of nonlinear sets.**
Ключевые слова: **Информационная безопасность, общие критерии, профиль защиты.**

I Ключевые аспекты создания системы безопасности информационных технологий

В связи с интенсивным использованием автоматизированных систем в различных областях жизнедеятельности все более актуальным становится вопрос обеспечения безопасности обрабатываемой информации.

При разработке системы безопасности информационных технологий (ИТ) одним из основных этапов является формирование совокупности требований безопасности для некоторых категорий объектов, направленных на противодействие идентифицированным угрозам в пределах определенной среды. Такая совокупность требований получила название профиля защиты (ПЗ). При создании ПЗ формируется набор функциональных требований и требований доверия, отображающих уровень доверия к объекту с точки зрения обеспечения безопасности.

В процессе формирования ПЗ возникает ряд трудностей, связанных с постановкой задачи обеспечения защиты и заданием нечетких требований к системе защиты информации, а также обоснованным выбором того или иного критерия и определения глубины его детализации. Одновременно с этим следует обратить внимание на отсутствие у критериев количественных характеристик, а также взаимозависимость между ними. При этом степень взаимозависимости между критериями может быть разной и меняться при изменении целей и среды безопасности изделия ИТ (в среду безопасности изделия ИТ входит как физическая среда, так и активы, подлежащие защите).

Одновременно с разработкой системы безопасности может возникнуть необходимость в проведении оценки, а также сертификации уже разработанной системы безопасности ИТ или ИТ в целом на соответствие определенным требованиям безопасности.

Решить поставленные задачи на мировом уровне призван международный стандарт ISO/IEC 15408-99 «Критерии оценки безопасности информационных технологий» или Общие критерии (ОК), содержащий систематизированные и иерархически связанные функциональные требования, требования доверия, а также рекомендации по применению ОК потребителями, разработчиками и оценщиками.

Аналогичный подход существует и в Украине. Нормативные документы системы технической защиты информации (НД ТЗИ), описывающие процесс создания комплексной системы защиты информации (КСЗИ) в автоматизированной системе (АС), предполагают разработку профиля защищенности, состоящего из набора критериев оценки защищенности информации. К сожалению, в украинском нормативном поле отсутствует документ, который бы описывал основные принципы формирования профиля безопасности АС. Причем желательно, чтобы подобная методика обладала свойством универсальности, то есть имела

возможность применения как с целью разработки защищенной АС, так и для проведения оценки уже разработанной системы обработки информации с точки зрения обеспечения требуемого уровня безопасности.

На этапе постановки задачи обеспечения защиты информации и формирования требований к системе защиты информации возникают также трудности, связанные с неопределенностью условий функционирования АС. Поэтому постановка задачи обеспечения защиты информации оказывается некорректной.

II Применение теории нечетких множеств для обеспечения безопасности ИТ

Задача обеспечения безопасности ИТ, как правило, не обладает свойством единственности решения. Известные математические модели, используемые для описания структуры, поведения и управления системой защиты информации, в условиях некорректной постановки задачи не дают желаемого результата. Поэтому необходима разработка новых, ориентированных на специфику процессов защиты информации методов и средств моделирования.

В связи с необходимостью обработки нечетко заданных величин и сложностью процесса принятия решения видится целесообразным проведение экспертной оценки с последующей обработкой полученной информации. Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистических переменных.

Используя данный подход и математический аппарат теории нечетких множеств применительно к обработке исходных данных и определению важности требований в данной работе предпринята попытка сформулировать задачу синтеза системы защиты информации и методы ее решения. Под задачей синтеза системы защиты информации будем понимать этап формирования профиля защищенности автоматизированной системы как основополагающий при создании КСЗИ. В общем виде задача синтеза сводится к формированию оптимального варианта реализации профиля защищенности, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на КСЗИ.

III Этапы формирования профиля защиты

В соответствии со стандартом ISO/IEC 15408-99, разработка ПЗ предполагает выполнение следующих действий.

1. Описать предполагаемую среду, связанную с безопасностью функционирования продукта или системы ИТ.
2. Определить стратегию противостояния каждой угрозе и сформулировать соответствующие цели безопасности. На этой стадии фактически определяется область действия ПЗ. Цели безопасности следует разделить на цели, достижение которых возлагается на объект оценки (ОО), и цели, достижение которых возлагается на среду.
3. Использовать каталог функциональных требований безопасности из части 2 ОК для спецификации функциональных возможностей, направленных на достижение целей безопасности для продукта/системы ИТ, а также для ИТ-среды.
4. Использовать каталог требований доверия к безопасности из части 3 ОК для спецификации компонентов доверия, направленных на обеспечение уровня доверия к безопасности, соответствующего целям безопасности.
5. Разработать логическое обоснование того, что выбранные функциональные компоненты и компоненты доверия к безопасности подходят для противодействия угрозам в предполагаемой среде.

Схематически процесс формирования профиля защиты приведен на рис. 1.

На этапе описания среды безопасности с учетом политики безопасности организации и на основе предположений о злоумышленнике формируется модель угроз, представляющая собой полный перечень всех возможных угроз, которые существуют или могут возникнуть в рассматриваемой ситуации. При составлении модели угроз учитывается также среда функционирования системы ИТ. Формирование модели угроз можно осуществить с применением автоматизированных диалоговых средств при одновременном участии экспертов. Для этого предполагается разработка специализированного опросника с несколькими вариантами ответов на каждый вопрос, который бы учитывал все возможные угрозы и все случаи применения того или иного критерия. Заполненный таким образом опросник позволяет эксперту получить информацию о:

- характеристиках угроз, существующих для данной системы и в данной среде;
- степени важности выполнения каждого критерия, что в дальнейшем необходимо для формирования требований доверия к безопасности;

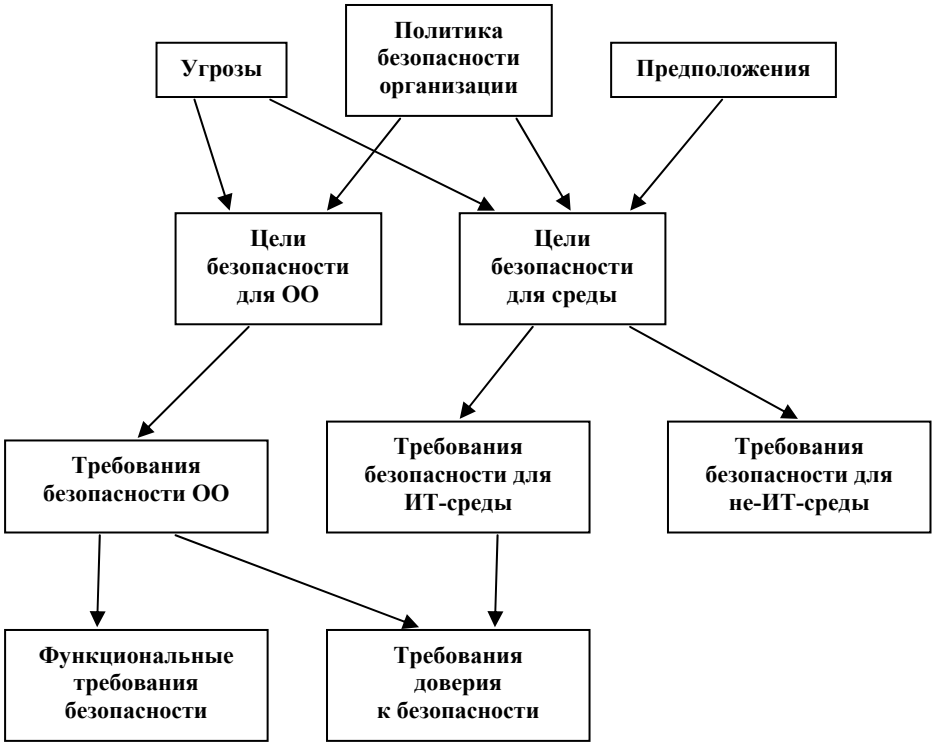

Рисунок 1 – Формирование профиля защиты

- степени взаимозависимости критериев, то есть степени необходимости выполнения одного критерия при выполнении другого для достижения требуемого уровня безопасности;
- заданном уровне качества СЗИ (выводится некий показатель качества СЗИ).

На основании экспертной информации, определяющей предпочтение того или иного показателя и информации о характеристиках угроз производится определение коэффициентов относительной важности выполнения j-го требования для устранения i-й угрозы. Из полученных таким образом коэффициентов формируется матрица лингвистических переменных, содержащая формализованное описание требований и среды безопасности.

Применяя к полученной матрице нечеткие арифметические операции, определяем важность требований, предъявляемых к СЗИ. Существует несколько методов определения важности требований, при этом на выбор метода будут влиять следующие основные факторы:

1. физическая сущность параметров и отношение между ними;
2. сложность проведения экспертизы и трудоемкость получения экспертной информации;
3. степень согласованности мнений экспертов;
4. трудоемкость обработки экспертных данных.

Параметры (требования) определяются исходя из заданных целей. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними, т. е. зависимости или независимости. Характер этой зависимости влияет на выбор метода.

Сложность и трудоемкость экспертизы определяется реальными условиями и возможностями ее проведения.

Степень влияния трудоемкости обработки экспертных данных будет зависеть от объема и уровня детализации входных данных.

На следующем этапе – этапе формулирования целей безопасности – с учетом вычисленного на этапе оценки уровня качества разрабатываются цели, для достижения которых и создается СЗИ. Для облегчения представления степени принадлежности требований безопасности заданному уровню качества используют понятие функции принадлежности. В теории нечетких множеств есть несколько методов построения функции принадлежности требований безопасности заданному уровню качества. Существуют методы построения функции принадлежности, основанные на статистических данных, на экспертных оценках, на

ранговых оценках, а также использующие параметрический подход. При выборе метода необходимо учитывать, как правило, сложность получения экспертной информации, достоверность экспертной информации, трудоемкость алгоритма обработки информации при построении функции принадлежности.

На следующем этапе проводится спецификация функциональных возможностей и компонентов доверия с целью формирования профиля защиты в зависимости и с учетом модели угроз, целей безопасности, а также полученных на предыдущих этапах данных о степени важности требований безопасности, их взаимозависимости и соответствии заданному уровню качества.

На заключительном этапе выполнения работ по созданию оптимальной СЗИ выполняется оценка СЗИ и выбор рационального варианта построения СЗИ.

При решении практических задач обоснования требований и оценки СЗИ возникает естественный вопрос рационального выбора метода определения весовых коэффициентов из числа существующих методов.

Принципиальными особенностями решения задачи выбора рационального варианта СЗИ, определяющим метод ее решения, являются:

- многокритериальность задачи выбора;
- не только количественное, но и качественное (нечеткое) описание показателей качества СЗИ, задаваемых в виде требований;
- при нечеткой постановке задачи влияние на выбор метода ее решения экспертной информации, определяющей предпочтение того или иного показателя.

Преимущественная особенность рассматриваемой задачи выбора – это качественный характер показателей, трактуемых как требования, задаваемые к СЗИ.

Выбор метода решения многокритериальной задачи зависит от того, в каком виде представлена экспертная информация о предпочтении показателей, а также от степени их важности (равная или различная важность требований).

В соответствии с формулировкой задачи, основными практическими этапами ее решения являются:

- разработка методики формирования и проведения экспертной оценки;
- разработка принципов и механизмов сбора и обработки экспертной информации о характеристиках угроз;
- разработка принципов и механизмов сбора и обработки экспертной информации с целью определения важности выполнения функциональных требований для устранения соответствующих угроз (выбор оптимального метода определения важности требований), а также расчет взаимозависимостных показателей;
- разработка математической модели и алгоритма выбора рационального варианта построения СЗИ (рационального задания требований, то есть формирования профиля) в соответствии с постановкой задачи как задачи нечеткого математического моделирования.

IV Выводы

Применение данной методики формирования ПЗ позволяет осуществить выбор оптимального варианта построения системы защиты информации на основе экспертной оценки требований и среды безопасности изделия ИТ, а также сформировать адекватный угрозам безопасности ПЗ для последующей его реализации в системе безопасности изделия ИТ. Одновременно с этим в силу своей универсальности возможно применение данного метода и для проведения оценки уже созданной системы безопасности ИТ на предмет выполнения возложенных на нее требований.

Литература: ***1.*** *ISO/IEC 15408-99 «Единые критерии оценки безопасности информационных технологий».* ***2.*** *НД ТЗИ 2.5-004-99.* ***3.*** *НД ТЗИ 2.5-005-99.* ***4.*** *Домарев В. В. Безопасность информационніх технологий. – М.: ДиаСофт, 2002. – 671 с.* ***5.*** *Общие критерии оценки безопасности информационных технологий: Учебное пособие. Перевод с английского Е. А. Сидак / Под ред. М. Т. Кобзаря, А. А. Сидака. – М.: ЦБИ, 2001. – 81 с.*