Island Parish // Human Relations. 1954. №7. Pp. 39-58. ***6.*** *Соціальні мережі – реальні загрози віртуального світу. – Режим доступу: http://ogo.ua/articles/view/2011-02-23/26490.html.* ***7.*** *Как социальные сети разрушают брак. – Режим доступу: http://letidor.ru/article/kak_sotsialnye_seti_razrushayu_138521/*

Владимир Бурячок, Андрей Орехов, Владимир Хорошко
Национальный Авиационный Университет

УДК 004.621.5

ОПТИМИЗАЦИЯ АРХИТЕКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СУВД

Аннотация: ***Приведена методика формирования профиля защищенности, которая позволяет осуществить выбор оптимального варианта построения системы комплексной защиты информации для информационного пространства системы управления воздушным движением (СУВД).***

Annotation: ***The article describes the method of forming the profile of security, which allows for selection of the optimal variant of building a system of complex information protection to the information space air traffic control system.***

Ключевые слова: ***система защиты информации, информационное пространство, система управления воздушным движением, профиль защищенности, архитектура.***

I Введение

Важным является вопрос оптимизации и унификации подходов к реализации мероприятий по обеспечению информационной безопасности как наиболее сложному и трудоемкому компоненту, обеспечивающему безопасность информации в системе управления воздушным движением. Особую роль играет при этом правильный выбор архитектуры системы защиты.

Целью защиты информации в СУВД является деятельность, направленная на предотвращение утечки ее по различным каналам и их блокирования.

Основной стратегией защиты информации является выбор основных и наиболее важных базовых системно-концептуальных положений и ориентиров при планировании, разработке и реализации этой стратегии. Основы стратегии защиты информации включают в себя необходимость использования двух терминологических понятий [1, 2]:

- стратегия технической защиты информации;
- стратегия безопасности защищаемой информации.

На практике в большинстве случаев системы защиты состоят из нескольких звеньев и рубежей. При попытке преодолеть защиту злоумышленник пытается использовать наиболее слабое направление или рубеж в этой системе. По этой причине итоговая прочность системы комплексной защиты информации (СКЗИ) будет определяться прочностью наиболее слабого направления или рубежа в этой системе.

II Основная часть

Так как итоговая прочность СКЗИ определяется прочностью наиболее слабого звена, рубежа или направления в этой системе, то, следовательно, если прочность слабого звена, рубежа или направления не удовлетворяет заданным и требуемым уровням, то это звено, рубеж или направление укрепляется или заменяется на более прочный.

Исходя из этого вероятность эффективной защиты информации при многорубежной системе определяется зависимостью:

$$P_{ИТ} = P_{СКЗИ_1} \cdot P_{СКЗИ_2} \cdot \ldots \cdot P_{СКЗИ_N},$$

где $P_{СКЗИ_N}$ - вероятность эффективной защиты *n*-го рубежа СКЗИ, *n* – порядковый номер рубежа.

Под задачей синтеза комплексной системы защиты информации понимается этап формирования профиля защищенности информационного пространства (ИП) как основополагающий при создании СКЗИ. В общем виде задача синтеза сводится к формированию оптимального варианта реализации профиля защищенности, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на создание СКЗИ информационного пространства СУВД. В соответствии со стандартом [3], известным также как "Общие критерии, разработка профиля защищенности" предполагается выполнение следующих мероприятий:

Мероприятие 1. Описать предполагаемую среду, связанную с безопасностью функционирования ИП СУВД.

Мероприятие 2. Определить стратегию противостояния каждой угрозе и сформулировать соответствующие цели безопасности. На этой стадии фактически определяется область действия профиля защищенности. Цели безопасности следует разделить на цели, достижение которых возлагается на объект, и цели, достижение которых возлагается на среду.

Мероприятие 3. Использовать каталог требований безопасности из второй части "Общих критериев, разработки профиля защищенности" для спецификации функциональных возможностей, направленных на достижение целей безопасности.

Мероприятие 4. Использовать каталог требований доверия к безопасности из третьей части "Общих критериев, разработки профиля защищенности" для спецификации компонентов доверия, направленных на обеспечение уровня доверия к безопасности, соответствующего целям безопасности.

Мероприятие 5. Разработать логическое обоснование того, что выбранные функциональные компоненты и компоненты доверия к безопасности подходят для противодействия угрозам.

Схематически процесс формирования профиля защищенности приведен на рисунке.

На этом этапе описания обнаружения безопасности с учетом политики безопасности ИП СУВД и на основании предположений о злоумышленнике формируется модель угроз, представляющая собой полный перечень всех возможных угроз, которые существуют или могут возникнуть в рассматриваемой ситуации.

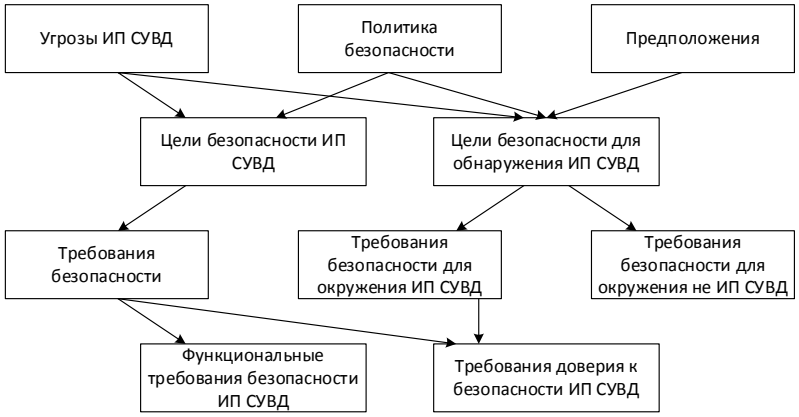

Рисунок – Формирование профиля защищенности

При составлении модели угроз учитывается также окружение функционирования ИП СУВД. Формирование модели угроз можно осуществить с применением автоматизированных диалоговых средств при одновременном участии экспертов. Для этого предполагается разработка специального вопросника с использованием нескольких вариантов ответов на каждый вопрос, который бы учитывал все возможные угрозы и все случаи применения того или иного критерия. Заполненный таким образом вопросник позволяет эксперту получить информацию о:

- характеристиках угроз, существующих и предполагаемых для ИП СУВД и в данном окружении;
- степени важности выполнения каждого критерия, что в дальнейшем необходимо для формирования доверия и безопасности;
- степени взаимодействия критериев, т. е. степени необходимости выполнения одного критерия при выполнении другого для достижения требуемого уровня безопасности;
- заданном уровне качества СКЗИ.

На основании экспертной информации, определяющей предпочтение того или иного показателя и информации о характеристиках угроз, производится определение коэффициентов относительной важности выполнения j-ого требования для устранения i-ой 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 системе защиты информации. Существует несколько методов определения важности требований. На выбор метода будут влиять следующие факторы:

- физическая сущность параметров и отношения между ними;
- сложность проведения экспертизы и трудоемкость получения мнений экспертов;

– трудоемкость обработки экспертных данных.

Параметры (требования) определяются исходя из заданных целей. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними. Характер этой взаимозависимости влияет на выбор метода.

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

На следующем этапе [2] (формулирования целей безопасности) с учетом вычисленного на этапе оценки уровня качества разрабатываются цели, для достижения которых и создается СКЗИ. Для облегчения представления степени принадлежности требований безопасности заданному уровню качества используют понятие функции принадлежности. В теории нечетких множеств есть несколько методов построения функции принадлежности. Существуют методы построения функции принадлежности, основанные на статистических данных, на экспертных оценках, на ранговых оценках, а также использующие параметрический подход. При выборе метода сложность получения экспертной оценки информации и её достоверность, а также трудоемкость алгоритма обработки информации учитываются при построении функции принадлежности.

На этом этапе проводится разработка спецификации функциональных возможностей компонентов СКЗИ. При этом учитывается степень доверия к этим компонентам. Причём спецификация позволяет сформировать профиль защищённости с учётом зависимости и моделей угроз безопасности ИП. Кроме того используются данные, полученные на предыдущих этапах: о степени важности предъявляемых требований к безопасности, их взаимозависимости и соответствии требованиям защищённости заданному уровню качества.

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

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

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

– многокритериальность задачи выбора;

– не только количественное, но и качественное (нечеткое) описание показателей качества СКЗИ, заданной в виде требований;

– при нечеткой постановке задачи влияние экспертной информации, определяющей предпочтение того или иного показателя.

Выбор метода решения многокритериальной задачи зависит от того, в каком виде представлена экспертная информация о предпочтении показателей, а также от степени их важности.

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

1) разработка методики формирования и проведения экспертной оценки;

2) разработка принципов, механизмов сбора и обработки экспертной информации о характеристиках угроз;

3) разработка принципов, 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 взаимозависимых показателей;

4) разработка математической модели и алгоритма выбора рационального варианта построения системы комплексной защиты информации в соответствии с постановкой задачи как задачи нечеткого математического моделирования.

III Выводы

Применение данной методики формирования профиля защищенности позволяет осуществлять выбор оптимального варианта построения СКЗИ на основе экспертной оценки требований и среды безопасности, а также сформировать адекватный угрозам безопасности профиль защищенности для последующей его реализации в системе безопасности. Одновременно с этим в силу своей универсальности возможно применение данного метода и для проведения оценки уже созданной системы безопасности на предмет выполнения заданных функций.

*Список використаної літератури**: 1.** Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К.: Арий, 2008. **2.** Штойер Р. Многокритериальная оптимизация. Теория, вычисления и приложения / Р. Штойер. – М.: Радио и связь, 1992. – 374 с. **3.** InternationalStandartISO/IEC 15408-99.*