УДК 004.056: 621.192

А.К. Орехов,
В.А.Хорошко

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

Рассмотрены проблемы и направления в решении вопросов защиты информации в СУВД. Применен комплексный подход к решению вопросов защиты информации. Рассмотрены методы разработки системы защиты и оценки эффективности их на основе частных и обобщенных показателей качества.

Ключевые слова: *защита информации, система, управление воздушным движением.*

Розглянуто проблеми та напрями у вирішенні питань захисту інформації в СУВД. Застосовано комплексний підхід до вирішення питань захисту інформації. Розглянуто методи розробки системи захисту та оцінки ефективності їх на основі приватних і узагальнених показників якості.

Ключові слова: *захист інформації, система, управління повітряним рухом.*

Problems and trends in the decision of an information security issues in the systems of air traffic control are considered. Complex approach to the decision of the information security issues is applied. Several methods for the development of the control system as well as for the estimation of their effectiveness on the basis of partial and generalized indicators of a quality are studied.

Keywords: *information security, system, air traffic control.*

Введение

Современные системы управления воздушным движением (СУВД) представляют собой сложную разветвленную локальную вычислительную сеть, осуществляющую решение широкого круга задач в реальном масштабе времени. Любое, даже незначительное вмешательство в процесс решения задач управления воздушной обстановкой (УВО) может привести к тяжелым последствиям. Поэтому необходимость защиты информации от несанкционированного доступа (НСД) в СУВД не вызывает сомнений. Эффективность системы защиты информации является неотъемлемой составляющей частью автоматизированной СУВД.

В настоящее время еще не сформирована единая теория защита сложных авиационных сетей, она находится в стадии формирования и становления, однако уже существует много теоретических подходов и практических решений по реализации защиты отдельных компьютерных систем и сетей. Важно четко представлять, что абсолютно защищенных систем нет. О защите и надежности этих систем можно говорить лишь с определенной вероятностью.

Система безопасности авиационной вычислительной системы УВД должна обеспечить заданный уровень защиты без значительного увеличения ее стоимости и снижения эксплуатационных характеристик.

Основная часть

Сформулируем основные цели защиты вычислительных систем УВД – обеспечения конфиденциальности (предотвращения несанкционированного доступа к информации), целостности (предотвращения несанкционированной модификации информации и самой системы) и действенности (предотвращение отказов при доступе к разрешенной информации) [1].

Для создания эффективной защиты вычислительной системы УВД необходимо провести анализ ее компонентов с точки зрения возможных попыток несанкционированного доступа к имеющейся в системе УВД информации. Вычислительная система УВД представляет собой совокупность аппаратных и программных средств, носителей информации, данных, каналов связи и обслуживающего персонала.

Структура ВС УВД определяет спектр методов ее защиты [2]:

– организационные методы, ограничивающие доступ обслуживающего персонала к конкретным элементам ВС УВД и самой УВД;

– методы ограничения доступа к каналам связи;

– аппаратные методы;

– программные методы;

Создание системы защиты – это комплексная задача, состоящая из нескольких этапов:

1. Анализ рисков – определение и оценка видов угроз, разработка и подбор оптимальных средств защиты.

2. Реализация политики безопасности – проведение мер по выполнению требований политики безопасности в вычислительной сети СУВД.

3. Поддержка политики безопасности – обеспечение функционирования реализации СЗИ в СУВД.

Одной из частей анализа требований к защите является выбор путей реализации политики безопасности. То есть, политика безопасности определяет правила, регулирующие организацию обработки информации в любой системе и на любом объекте. Для описания механизма защиты строится модель (см. рис. 1) [3], описывающая состояние СУВД, переходы системы из одного состояния в другое, а также как состояния и переходы считаются безопасными. При разработке модели применяется широкий спектр математических методов.

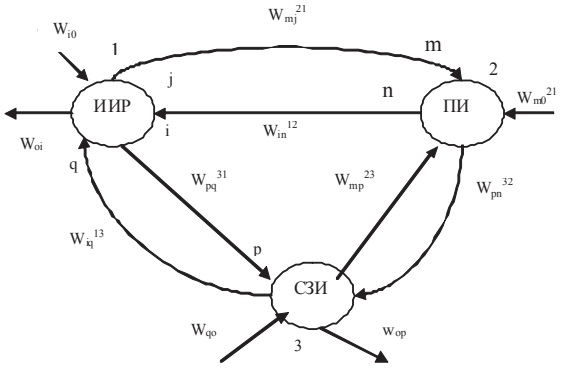

Рис. 1. Модель – граф взаимосвязи СЗИ СНИР и ПМ СУВД

Различают два вида политики безопасности [4]: избирательная и полномочная. Основой избирательной политики безопасности является избирательный контроль доступа операторов (пользователей) вычислительной сети СУВД и ее объектам на основе идентификации субъектов и групп, к которым они принадлежат. Под субъектами СУВД понимаются такие, которые определяют условия пользования, хранения, обработки и пересылки информации. Это администратор системы, пользователь (оператор), системные и прикладные программы.

Объекты – это файлы, директории и аппаратные элементы ВС и СУВД.

Избирательный контроль доступа (ИКД) направлен на ограничение доступа субъекта к защищенным объектам и элементам системы. Множество таких объектов, типы доступа к ним могут изменяться в соответствии с критериями, существующими в данной системе. Контроль за изменениями этих критериев также являются задачей НКД.

Основным инструментом, с помощью которого НКД, выполняет свои задачи, является матрица контроля доступа (МКД) – матрица, определяющая типы доступа, разрешенные для каждого из субъектов при обращении к любому из объектов.

Полномочная политика базируется на понятии многоуровневой защиты. Каждому объекту в системе приписана метка критичности, определяющая ценность содержания в нем информации: каждому субъекту приписан уровень прозрачности – метка, определяющая максимальное значение метки критичности объектов, к которым данный объект имеет доступ. Для разрешения доступа осуществляется сравнение метки критичности объекта и уровня прозрачности объекта.

Необходимо отметить, что избирательный контроль доступа эффективней полномочного, поэтому он должен применяться как основной, дополненный полномочным контролем, придающий требованиям безопасности системы УВД иерархически упорядоченный характер.

Контроль доступа обеспечивает достаточно надежную защиту информации в СУВД от НСД. Однако, учитывая тот факт, что система УВД представляет собой разветвленную информационно-вычислительную сеть с множеством каналов связи, существует опасность утечки информации при ее передачи по каналам связи. При этом может быть получена информация не только о содержимом объекте, но и о его состоянии, атрибутах и т.д.

Следовательно, необходим анализ потоков информации в системе, определение возможных путей ее утечки, разработка правил, регулирующих информационные потоки в системе и реализация контроля информационных потоков [5].

Применение избирательного метода контроля в сочетании с полномочным, а также контроль информационных потоков обеспечивает безопасность ВС УВД только при правильной реализации разработанной политики безопасности.

Важнейшим условием при этом является надежная защита всех системных и программных средств, отвечающих за реализацию политики безопасности. Все средства защиты и контроля должны быть реализованы в достоверной информационной базе.

Другим важным механизмом реализации политики безопасности является концепция защищенной области. Он заключается в объединении объектов по их местонахождению, хранимой информации, защите и внутренней структуре.

Управление осуществляется областью в целом с помощью специального программного обеспечения, доступ к отдельным объектам запрещен.

Поэтому необходимо для оценки качества механизмов политики безопасности разработать критерии качества.

Для оценки качества функционирования ВС СУВД и самой СУВД необходимо определить критерии, позволяющие осуществлять эту оценку.

Зададим на основании проведенной классификации параметров модели [1, 3], которые необходимы для дальнейшего исследования системы: средняя продолжительность периода передачи (*t*пер); средняя продолжительность периода работы программы (*t*ср); средняя длина информационного пакета $(1/\theta)$ и индекс эффективности – производительность системы в данный момент времени Π_t. Соотношения между θ и V выводится из операционных характеристик архитектуры СУВД, причем полученные как отношение θ, V и $t_ф$ и $t_{пер}$ характеризуют рабочую нагрузку модели (g), нагрузку задаваемую BC (g_{BC}) и программой ($g_ф$).

Так как рассматриваемая модель предназначена для решения конкретного набора задач по УВД, то относится к многокритериальной задаче оптимизации. Характерной особенностью решения этого класса задачи оптимизации является наличие конечного числа частных критериев, соответствующих частным программам системы. В отдельных случаях удается сформировать также глобальный критерий, соответствующий всей системе в целом. Это возможно в таких случаях, когда существует единая цель в решении задач ВС СУВД, а частные критерии характеризуют задачи подсистем, функционирующих в интересах системной задачи.

Поэтому качество функционирования ВС СУВД описывается совокупность частных критериев, которые необходимо минимизировать:

$$\overline{K} =< K_1, \mathrm{K}_2, ..., \mathrm{K}_\mathrm{m} > .$$

Найдем относительные отклонения частных критериев от экстремальных (минимального и максимального) значений:

$$\Delta K_i = \frac{K_i - K_{i\max}}{K_{i\max}},\ i = \overline{1,\mathrm{m}} \qquad (1)$$

Тогда выбранный элемент СУВД будет описываться по совокупности частных критериев K_i, $i = \overline{1,\mathrm{m}}$, если он характеризуется совокупностью относительно отклонений ΔK_i, имеющих наименьшее значения. При этом обозначим оптимальной оптимальный вариант вычислительного модуля ВС или элемент СУВД и в формальном виде эту задачу запишем в следующем виде:

$$\begin{aligned} &\Delta K(BM_o) < \mathrm{K}_{\max}, \\ &BM, BM_o \in M_{cg} \end{aligned} \qquad (2)$$

где $\mathrm{K}_{\max} = \max(\Delta K_i)$; $i = \overline{1,\mathrm{m}}$ – наибольшее из относительных отклонений, рассчитываемых по формуле (1); M_{cg} – множество вычислительных модулей ВС или

СУВД (строго доступных), удовлетворяющих совокупности условий применения и ограничений на структуру и значения основных параметров.

Предложенный критерий отличается от известных тем, что позволяет производить оценку ВС СУВД в диапазоне возможных отклонений частных критериев и тем самым дополнительно учитывает степень ухудшения одних параметров за счет улучшения других. Однако при $K_{imin} << K_{i\max}$ использование этого критерия может привести к тому, что предпочтение может быть отдано ВМ ВС или элементу СУВД, который при незначительно лучшем (меньшем) значении одного показателя качества обладает значительно более худшими остальными показателями по сравнению с соответствующими показателями качества других ВМ ВС или элементами СУВД. В этом случае рассматриваемый критерий приобретает те же недостатки, которыми обладают и известные критерии.

Минимальный критерий (2) можно представить в виде:

$$K_p = f_p(K_1, K_2, ..., K_i, ...K_m) = \min, \quad BM \in M_{cg}, \tag{3}$$

где $$f_p = (K_1, K_2, ..., K_i, ...K_m) = \max \frac{K_1 - K_{1\min}}{K_{1\max}}, ..., \frac{K_i - K_{i\min}}{K_{i\max}}, ..., \frac{K_m - K_{1\min}}{K_{1\max}}. \tag{4}$$

Модуль BM_o определяется решением задачи (3, 4) и является оптимальным. Из выражения (3) следует, что минимальный критерий можно считать разновидностью критерия, основанного на минимизации результирующей целевой функции, вид которой соответствует выражению (4).

Кроме того, из зависимостей (3) и (4) видно, что этот критерий обеспечивает наименьшее значение из совокупности наибольших нормированных показателей качества. Поэтому все частные показатели качества должны быть приведены к стандартному виду. И, следовательно, показатель качества $\underline{K_i}$ будет считаться стандартным, если он удовлетворяет условию $K_i \geq 0$, где $i = \overline{1, m}$. Если же показатель качества не является стандартным, то его всегда можно привести к этому виду.

И на основании разработанных критериев проведем оценку эффективности применения средств защиты информации в СУВД.

Оценка эффективности средств защиты информации в СУВД возможна на основании анализа обобщенной модели – графа взаимодействия СЗИ с источником информационных ресурсов (ИИР) и пользователя информации (ПИ) при рассмотрении соответствующих свойств системы и использовании данных [1, 3].

Поскольку частными показателями эффективности функционирования СЗИ СУВД могут быть отдельные ее “свойства” или их совокупность, которые описываются уравнениями:

$$a_I^{\beta} = \sum_{\substack{\beta \in h \\ \gamma \in \varphi}} a_N^{\varphi} w_{IN}^{\beta Y} + \sum_{\beta \in h} a_{IO}^{\beta} + \sum_{\substack{I \neq J \\ \beta \in k}} a_j w_{jI}^{\beta h}, \tag{5}$$

где I, j – точка входа и выхода системы β $(I \neq j)$; правая часть в порядке следования представляет собой произведения обобщенных множеств переменных

произвольной β – системы на операторы *{W},* характеризующие способы реализации этих свойств, транслируемые соответственно *N*-точками выхода системы, внешней среды (0) и φ-точками внутренних переменных *h*- системы.

Для оценки показателя эффективности преобразуем обобщенную в соответствии с рис. 1.

Проанализировав взаимосвязь между СЗИ СУВД, ИИР и ПИ, составим семейство уравнений, описывающих взаимосвязь свойств систем ПИ, ИИР и СЗИ:

;

$$a_m^2 = \sum_{m=1-4} a_{mo}^2 w_{mo}^{20} + \sum_{m=1,4} a_2^3 w_{m2}^{23} + \sum_{m\neq n=1-4} a_n^2 w_{nm}^{22} + \sum_{m=1-4} a_1^3 w_{m1}^{23}; \quad (6)$$

$$a_p^3 = \sum_{p=1-3} a_3^1 w_{p3}^{31} + \sum a_{po}^3 w_{po}^{30} + \sum a_q^3 (w_{qp}^{33})^{-1} + \sum_{m=1,2,4} a_n^2 w_{pn}^{32};$$

$$a_3^1 = a_3^3 w_{33}^{13}; \qquad a_3^3 = \sum_{m=1,2,4} a_m^2 w_{3m}^{32}.$$

Анализ выходных переменных систем согласно рис. 1 при помощи выражения (5) дает возможность определить частные показатели эффективности функционирования СЗИ СУВД при выполнении самостоятельных (w_{pq}^{33}) или межсистемных (w_{32}^{13}, w_{33}^{31} и др.) функций по связи с внешней средой.

В конечном итоге эффективность функционирования СЗИ СУВД будет определяться возможностями *(W)*, т.е.:

$$Э_{СЗИСУВД} = f[a_m, a_n, w_{in}, w_{mj}, w_{qn}, w_{mq}, ...]. \quad (7)$$

Выражения для обобщенной эффективности СЗИ СУВД для рассматриваемого уровня взаимодействия систем примет вид:

$$Э^{(1)}{}_{СЗИСУВД} = \sum_{\xi\neq r} H_{32} H(W_{\xi r}) / \sum H_{\varsigma r}, \quad (8)$$

где $\varsigma = r = i, j, m, n, p, q, O$; $H_{\varsigma r}$ – коэффициенты, определяющие потребность в реализации задач СЗИ ($H_{\varsigma r} = 1$), их значимость. Отсутствие такой потребности характеризуется величиной $K_{\varsigma r} = 0$.

Приведенные выражения дают более точную оценку эффективности СЗИ, чем вероятностные показатели, которые рекомендуются в работах [1, 2, 5], а применения ПЭВМ позволяет этот процесс автоматизировать и повысить точность определения эффективности.

Выводы

Организация защиты ВС СУВД – это единый комплекс мер, который учитывает все аспекты процесса обработки, применения и распространения информации.

Рассмотрены проблемы относительно пути решения вопросов защиты информации в вычислительной сети СУВД. Применен комплексный подход к решению проблемы и приведена методика разработки системы защиты информации. А также рассмотрен метод и приведена методика оценки эффективности системы защиты информации на основе определения частных и обобщенных показателей качества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Ленков С.В.* Методы и средства защиты информации : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008.

2. Захист інформації в системі організації повітряного руху / І.С. Биковцев, В.С. Демянчук, В.О. Клименко, В.О. Хорошко та ін. – К. : ДП ОПР України, 2008. – 236 с.

3. *Хорошко В.А.* Модель системы защиты информации / Хорошко В.А. // Захист інформації. – № 1, 1999. –С. 5–11.

4. *Бурячок В.Л.* Політика інформаційної безпеки / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко. – К. : ПВП "Задруга", 2014. – 222 с.

5. Методы прогнозирования защищенности ведомственных систем связи, основанные на концепции отводного канала / В.Г. Лихограй, А.А Стрельницкий, А.И. Цопа, В.М. Шокало. – Харьков: КП "Городская типография", 2011. – 502 с.

Отримано 3.09.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.