УДК 621.3

СПОСОБ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С.И. Попов, С.Ю. Рослов

Рассмотрен способ оценки параметров (показателей) эффективности информационной безопасности (ИБ) автоматизированных систем управления специального назначения (АСУ СН). Приведено обоснование количественного показателя ИБ, который, в частности, не противоречит требованиям руководящих документов по ИБ в автоматизированных системах (АС)

Ключевые слова: оценка параметров, автоматизированная система, безопасность

В настоящее время благополучие и даже жизнь многих людей зависят от обеспечения ИБ множества компьютерных систем обработки информации, а также контроля и управления различными объектами. К таким объектам (часто их называют критическими) можно отнести информационно-телекоммуникационные системы специального назначения, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, а также системы обработки и хранения сведений, составляющих государственную тайну. Для нормального и безопасного функционирования подобных систем необходимо поддерживать их безопасность и целостность.

Под АСУ СН понимаются системы управления двойного назначения, военные, экологически опасных производств, транспорта, связи, финансово-кредитной сферы и т.д., в которых размеры ущерба или других последствий, возникших в результате нарушения их работоспособности, сбоев и отказов в работе, оказываются неприемлемыми, а порой и катастрофическими для общества.

Широкое применение локальных, корпоративных и глобальных сетей с использованием стандартных (открытых) протоколов передачи данных еще более усугубляет проблему обеспечения ИБ, так как создаются возможности удаленного НСД к данным и вычислительному процессу.

В связи с этим возникает весьма актуальная и практически значимая задача защиты информационных процессов в АСУ СН от НСД, получения, модификации и искажений программ и данных [1-8].

Для обеспечения ИБ используются специальные системы защиты информации (СЗИ), входящие в АСУ СН в качестве проблемно-ориентированной подсистемы и содержащие технические и программные средства защиты.

Можно выделить следующие основные направления обеспечения ИБ АСУ СН, создаваемых из ненадежных (уязвимых) элементов [1, 9]:

- обеспечение безопасности данных, т.е. наделение защитой данных методами криптографии как их внутренним свойством. Фактически сегодня шифрование - единственная гарантия защиты данных, особенно при их хранении и передачи по каналам связи. Однако, оно не всегда приемлемо из-за снижения скорости обработки данных, неудобств их интерпретации и отображения, высокой стоимости оборудования, сложности и уязвимости (опять же, «человеческий фактор») систем обеспечения;
- обеспечение безопасности аппаратных средств (проведение спецпроверок, специсследований и программного обеспечения (дополнительное тестирование на отсутствие скрытых и недокументированных функций);
- создание программно-аппаратных средств защиты от НСД (для отдельных рабочих мест, сетевых и межсетевых);
- комплексирование перечисленных выше направлений с организационно-техническими мерами в рамках системы обеспечения ИБ АСУ СН.

При реализации этих направлений функция обеспечения ИБ рассматривается как дополнительная по отношению к информационно-технологическому процессу АСУ СН и проектируется («навешивается») после ее создания. Как следствие, в соответствующие системы ИБ закладывается так называемый принцип «изощренного замка» [2,4]: для заданного информационно-технического процесса, аппаратных и программных средств его реализации определяются места уязвимости и угрозы безопасности, которым противопоставляется

Попов Сергей Иванович – ВИПС ФСО РФ, соискатель, тел. 8-(910)3496739
Рослов Сергей Юрьевич – ВИПС ФСО РФ, соискатель, тел. 8-(903)8551157

адекватный механизм защиты информации (ЗИ.) Если этот механизм «взламывают», то его усложняют, и т.д.

Основной целью средств и систем защиты информации (СЗИ) АСУ СН является обеспечение нейтрализации потенциальных угроз информации в АСУ СН.

На основе анализа [1-3] можно сделать следующий вывод, что основным показателем эффективности функционирования АСУ СН, работающей в условиях жестких временных ограничений и воздействия НСД злоумышленника, является длительность цикла управления ($T_{управления}$), который характеризует степень достижения цели функционирования АСУ СН по своему назначению.

Использование в качестве показателя эффективности АСУ СН длительности цикла управления $T_{управления}$ позволяет учитывать влияние уровня ИБ на качество функционирования системы. В условиях информационного воздействия злоумышленника путем реализации попыток НСД время, затрачиваемое на цикл управления в АСУ СН, будет увеличиваться за счет отвлечения ресурсов на противодействие возникшим угрозам ИБ. Величина этого увеличения определяется степенью эффективности применяемых средств и способов ЗИ. Если эта эффективность неадекватна уровню угроз, то возможное искажение, хищение или утрата информации приведет к значительному возрастанию $T_{управления}$ или невозможности, в крайнем случае, функционирования АСУ СН. При успешной реализации функции СЗИ, это увеличение $T_{управления}$ будет определяться затраченными программными и аппаратными ресурсами на осуществление задач ЗИ, что требует разработки моделей и методик оценки показателей эффективности применяемых СЗИ и выбора оптимальных её параметров с учетом ограничений на допустимый прирост $T_{управления}$

При рассмотрении процессов цикла управления в АСУ СН рассматриваются вероятностно-временные характеристики цикла управления и его этапов в конкретных видах управляющей деятельности, например процессов взаимообмена различными видами оперативной информации, процессов информационно-расчетного обеспечения и т.д. В формализованном виде данный показатель можно представить в следующем виде:

$$T_{управленияя} = F(P_t, V, \lambda, E) \qquad (1),$$

где, F – функциональная зависимость;

P_t – вероятностно-временные характеристики выполнения этапов или элементов цикла управления;

V – объем массивов информации, используемых в цикле управления и необходимой для принятия решений;

λ – интенсивность потоков обмена для различных этапов и элементов цикла управления;

E– показатель ИБ, который характеризует защищенность АСУ СН от преднамеренного НСД злоумышленника.

Анализ процессов функционирования АСУ СН и СЗИ в них позволяет сделать вывод [1-3], что достижение минимально возможного в конкретных условиях (оптимального) $T_{управления}$ возможно при выделении такого объема ресурсов, которые обеспечивают необходимый уровень защищенности информации (Е) в АСУ СН от попыток НСД со стороны злоумышленника, определяемый на основе назначения и требований к конкретной АСУ СН, а с другой стороны, отвлекаемые этой целью ресурсные затраты не должны приводить к увеличению длительности цикла управления.

Определение необходимого соотношения рассмотренных ресурсов требует построения моделей, описывающих функционирование АСУ СН и проведение на их основе имитационного моделирования, что выдвигает задачу разработки соответствующего математического обеспечения.

В [8] представлена иерархия задач ЗИ решаемых СЗИ в АСУ СН.

Для задачи первого уровня наиболее целесообразной формой показателя эффективности является вероятность защиты от НСД $P^{(НСД)}$.

Для совокупности задач второго уровня: (предупреждение условий, благоприятных возникновению угрозы; предупреждение появления угроз; поиск, обнаружение и обезвреживание источников угроз; нейтрализация воздействий угроз; обнаружение воздействий угроз; локализация воздействий угроз; восстановления информации после воздействия угроз) наиболее целесообразной формой показателя эффективности являются соответствующие времена [8]:

$\tau^{(1.1)}$ - время предупреждения условий, благоприятных возникновению угрозы;

$\tau^{(1.2)}$ - время предупреждения появления угроз;

$\tau^{(1.3)}$ - время поиска, обнаружения и обезвреживания источников угроз;

$\tau^{(1.4)}$ - время нейтрализации воздействий угроз;

$\tau^{(1.5)}$ - время обнаружения воздействий угроз;

$\tau^{(1.6)}$ - время локализации воздействий угроз;

$\tau^{(1.7)}$ - время восстановления информации после воздействия угроз.

Принимая во внимание, что с точки зрения применения СЗИ в АСУ СН наибольший интерес для исследования представляют соотношения ее временных характеристик и временных характеристик процесса ее вскрытия, в качестве основы для конструирования показателя эффективности СЗИ в АСУ СН условимся использовать время обеспечения ею защитных функций [5]. При этом под временем $\tau_{(di)}$ обеспечения защитных функций СЗИ в АСУ СН в дальнейшем условимся понимать время с момента обращения к СЗИ в АСУ СН до окончания реализации ею своих функций по данному обращению. Защитные функции СЗИ в АСУ СН считаются реализованными своевременно, если время $\tau_{(di)}$ не превышает некоторой максимально допустимой величины $\tau_{(m)}$, обусловленной стратегией вскрытия СЗИ в АСУ СН злоумышленником, т.е. при выполнении неравенства [5-8]:

$$\tau_{(di)} \le \tau_{(m)} \qquad (2)$$

Максимальное время выполнения защитной функции СЗИ ($\tau_{(m)}$), которое указано в разделе «Требования по НСД», при разработке АСУ СН.

Тогда показатель (Е) имеет следующий вид:

$$E=P\ (\tau_{(di)} \le \tau_{(m)}), \qquad (3)$$

Способ оценки показателя защищенности АСУ СН (Е) базируется на использовании аппарата математического моделирования СЗИ как сети массового обслуживания.

Литература

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994. - 400 с.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 2. - М.: Энергоатомиздат, 1994. - 176 с.
3. Зегжда П.Д. Теория и практика обеспечения информационной безопасности. - М.: Издательство «Яхтсмен», 1996.- 192 с.
4. Львович Я.Е., Скрыль С.В. Распределенная защита информации как фактор повышения эффективности мер по борьбе с преступлениями в сфере компьютерной информации. // Региональный научно-технический вестник «Информация и безопасность», Выпуск 3. – Воронеж: ВГТУ, 1998. - с.125-129.
5. Скрыль С.В. Показатель эффективности защиты информации в автоматизированных системах. // Материалы Международной конференции “Информатизация правоохранительных систем”. Ч.2. - М.: Академия управления МВД России. 1997. с. 36-38.
6. Кочедыков С.С., Потанин В.Е., Рогозин Е.А., Скрыль С.В., Паринова Л.В.. Об одном способе решения задачи оптимального распределения временного резерва в информационно-телекоммуникационных системах в интересах обеспечения информационной безопасности. // Региональный Научно-технический вестник “Информация и безопасность”, Выпуск 1. – Воронеж, ВГТУ, 2000, с.40-44.
7. Завгородний М. Г., Махинов Д. В., Скрыль С. В. Способ формирования аналитических выражений для оценки своевременности реакции подсистемы защиты информации. // В сборнике «Прикладные вопросы защиты информации», Воронеж, Изд-во Воронежской высшей школы МВД России, 1996. - с.
8. Львович Я.Е., Рогозин Е.А. Способы комплексной оценки эффективности при проектировании программных систем защиты информации в автоматизированных системах управления критических приложений // Прикладные задачи моделирования и оптимизации: Сб. науч. тр. Воронеж: Изд-во ВГТУ, 2000. С.31-39.
9. Герасименко В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений. // Региональный научно-технический вестник «Информация и безопасность», Выпуск 4. – Воронеж: ВГТУ, 1999. - с.66-67.

Воронежский институт правительственной связи (филиал) Академии Федеральной службы охраны Российской Федерации

WAY OF THE ESTIMATION OF INFORMATION SAFETY OF THE AUTOMATED CONTROL SYSTEMS OF SPECIAL ASSIGNMENT

S.I. Popov, S.U. Roslov

The way of an estimation of parameters of efficiency of information safety (IS) of the automated control systems of special assignment (MIS SA) is considered. The substantiation of quantity indicator IS which on IS in the automated systems, in particular, does not contradict requirements of supervising documents is resulted

Key words: estimation of parameters, the automated system, safety