УДК 65.012

В.Я. ПЕВНЕВ

Харьковский национальный университет внутренних дел, Украина

ЭФФЕКТИВНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАМКНУТЫХ СИСТЕМ

Предложены определения основных терминов, употребляемых в работе. Анализируются возникающие угрозы информационной безопасности замкнутых систем и методы их оценки. Рассматриваются возможные критерии эффективности информационной безопасности. Анализируются каналы утечки информации, характерные для закрытых систем и методы противодействия навязыванию ложных данных. Предлагается комплексный показатель определения эффективности и способ его вычисления.

Ключевые слова : *эффективность, информационная безопасность, критерии эффективности, показатель эффективности, замкнутая система, каналы утечки.*

Введение

Информационной безопасности (ИБ) в настоящее время уделяется много внимания на всех уровнях, начиная от государства и заканчивая физическими лицами. Особую актуальность ИБ приобретает в связи с проникновением технических средств обработки и передачи данных практически во все сферы человеческой деятельности. Несмотря на большую практическую значимость, в литературе практически отсутствуют сведения о ИБ замкнутых систем (ЗС), хотя такие системы играю огромную роль в производственном цикле. Особое значение приобретает оценка эффективности ИБ (ЭИБ). В [1] говорится, что в настоящее время отсутствуют количественные методы оценки ЭИБ. Применение качественных методов оценки на сегодняшний день является единственным способом получить представление о реальном уровне защищенности информационных ресурсов системы. Такой подход к определению ЭИБ не позволяет объективно оценить разрабатываемые системы защиты информационных систем.

Целью работы является рассмотрение предложенных критериев ЭИБ ЗС, каналов утечки и внешнего воздействия на ЗС и выработка комплексного показателя определения эффективности.

1.Основная часть

1.1. Терминология

Прежде чем рассматривать вопрос, вынесенный в заголовок статьи, необходимо дать определения некоторых терминов, которые используются в предлагаемой работе. Автору наиболее близка следующая формулировка информационной безопасности: ИБ это свойство системы противостоять несанкционированному снятию и модификации информации [2].

Под несанкционированным снятием понимается получение информации, к которой у абонента нет доступа.

Под несанкционированной модификацией понимается изменение информации, которое приводит к нарушению ее целостности. Следует отметить, что целостность, в общем случае, это не только полученная информация в исходном виде, но и ее полнота.

Замкнутой системой, с точки зрения ИБ, будем называть такую систему, в которой все элементы, включая оконечные устройства и составляющие каналов связи, находятся на охраняемой территории.

Под эффективностью информационной безопасности будем понимать степень соответствия результата проведенных мероприятий по обеспечению ИБ поставленной цели.

1.2. Критерии эффективности

Какие угрозы возникают для ИБ ЗС? Во-первых, это незаконное снятие информации, которая циркулирует в контуре управления и в информационном контуре. Во вторых, это несанкционированная модификация информации, поступающей с различных датчиков или направляемой к исполнительным устройствам. Если в состав ЗС входит интеллектуальная система какого-либо назначения, то это несанкционированное изменение элементов базы данных и / или знаний. Кроме несанкционированных воздействий необходимо оценить возможность природных факторов, которые могут нанести значительно больший ущерб, чем несанкционированное снятие информации.

Каким образом можно оценить такие угрозы? Совершенно очевидно, что все оценки будут вероятностными. Нам неизвестно, какими устройствами будут обладать потенциальные нарушители, какие цели они поставят перед собой. Поэтому, для оценки ИБ ЗС необходимо выработать критерии эффективности. Эти критерии необходимо согласовывать на стадии проектирования системы между представителями заказчиков и разработчиков. При этом возможны различные подходы, среди которых выделяются два: при отсутствии жестких ограничений на ресурс, выделяемый для защиты информации и при заданном ресурсе [3].

В зависимости от назначения системы эти критерии могут быть различными:

– минимизации вероятности несанкционированного снятия и / или модификации информации;

– минимизации затрат на построение системы защиты при заданной вероятности противодействия несанкционированным действиям нарушителей;

– максимизации устойчивости к внешним воздействиям;

– минимизации времени восстановления при сбоях и отказах, вызванных нарушением информационных ресурсов.

Совершенно очевидно, что при разработки новых систем можно использовать и другие критерии, отличающиеся от предложенных.

1.3. Каналы утечки

Следует обратить особое внимание на комплексный подход при разработке системы защиты, который должен включать как методы построения системы защиты, так и определения эффективности разработанной системы. При оценке ЭИБ ЗС следует учитывать особенности таких систем. К таким особенностям в первую очередь следует отнести невозможность проникновения нарушителю в компьютерную систему. Внешние воздействия на систему возможны лишь в виде помех, что может привести к сбоям в ее работе, или навязывании ложных импульсов, которые могут привести к выработке неадекватным реальной ситуации управляющих сигналов. В худшем случае внешнее воздействие может привести к разрушению всей системы.

При рассмотрении каналов утечки информации следует выделять [4]:

– визуально-оптические;
– акустические;
– электрические;
– материально-вещественные.

Основным каналами утечки информации в ЗС являются побочные электромагнитные излучения, визуально-оптический и акустический канал. Автор сознательно уходит от анализа таких составляющих каналов утечки информации, как наведенная ЭДС, различного рода закладные устройства и других, нейтрализовать которые необходимо на этапе проектирования и с помощью различных организационных мероприятий, что достаточно просто осуществить, памятуя о том, что разговор идет о ЗС. Построение ЗС предполагает и наличие автономного источника питания, которое нейтрализует возможность нарушение целостности информации с помощью нарушения электропитания [5]. Ввиду тестирования программного обеспечения на этапе ввода в эксплуатацию и отсутствия внешних связей исключается возможность внедрения вредоносных программ и возникновения различных конфликтных ситуаций. В работе так же не рассматривается человеческий фактор, хотя он является одним из основных при определении ИБ.

Кроме этого, необходимо сделать еще одно ограничение. Оно заключается в рассмотрении ИБ с точки зрения принятия решения. Качество принятия решения обеспечивается целостностью информации. Адекватность выработанного решения будет зависеть от программного продукта, количества информации, которая учитывается при выработке решения, времени, выделяемого на принятие решения, опыта лица, принимающего решения и т.д. Эта проблема не рассматривается в данной работе.

Когда рассматриваются каналы утечки, главной задачей становится минимизация возможностей снятия информации. Другими словами необходимо понизить уровень незаконно снимаемого сигнала так, что бы он ни дал злоумышленнику никакой полезной информации. Нормой эффективности принятых мер защиты в этом случае считается максимально допустимое значение контролируемого параметра на границе охраняемой территории, где уже возможно нахождение средств разведки [6] Этого можно достичь как за счет организационных, так и технических мероприятий.

Более сложным при обеспечении ИБ становится вопрос внешнего воздействия на различные системы, в том числе и замкнутые, которое может быть различным в зависимости от типа электромагнитных помех. Помехи могут быть узко- и широкополосными, высоко- и низкочастотными, направленными, заградительными, в виде мощного электромагнитного импульса (ЭМИ) [5].

Результаты действия помех в системах связи нейтрализуются с помощью помехозащищенного кодирования. Однако в ЗС такой вид кодирования практически не применяется.

Особую сложность представляет защита от ЭМИ. Импульсные электромагнитные поля являются причиной возникновения помеховых токов

и напряжений, которые, проникая в радиоэлектронные средства, приводят к выходу их из строя. Проникновение помех происходит по вполне конкретным путям, которые в соответствии с [7] определены как опасные тракты. В ЗС к ним можно отнести межблочные кабельные и проводные электрически короткие линии связи, цепи электропитания, системы заземления и общих точек, корпуса-экраны.

В настоящее время создан новый вид вооружения – электромагнитное оружие [8]. С помощью ЭМИ можно оказать поражающее воздействие на элементную базу информационной системы, даже если она находится в выключенном состоянии.

Главным видом противодействия возможным каналам утечки и внешнего воздействия на ЗС на сегодняшний день является реализация защитных мероприятий на этапах проектирования и конструирования информационных систем.

1.4. Комплексный показатель эффективности

Для оценки ЭИБ необходимо ввести комплексный показатель (КП), составные части которого были бы пропорциональны степени влияния каждого вида угроз на конечный результат. Подобные задачи достаточно сложны [9], но в нашем случае сложность увеличивается многократно. Это обуславливается назначением ЗС, которые, как правило, являются стратегически важными. Величина КП и порядок его вычисления будет определяться выбранным критериям. Величина каждого показателя будет зависеть от многих факторов, например, от международной обстановки. В мирный период основной угрозой для ИБ будет утечка информации. В военный период большая вероятность деятельности, направленной на разрушение ЗС.

При разработке КП необходимо провести ранжирование его составных частей в зависимости от возможности нарушения ИБ в зависимости от вида угроз. В общем случае величина КП может быть определена с помощью выражения (1)

$$K = \sum_{i=1}^{n} k_i * (1 - p_i) \qquad (1)$$

где k_i - весовой коэффициент;

p_i - вероятность нарушения ИБ по i-му виду угроз.

При этом необходимо учитывать, что

$$\sum_{i=1}^{n} k_i = 1$$

Величина весовых коэффициентов k определяется экспертами и зависит от конкретного объекта: его расположения на местности, степени выполнения организационных и технических мероприятий по защите информации и др.

Следует отметить и тот факт, что величины весовых коэффициентов k не являются постоянными на всем рассматриваемом интервале времени, и во многом будут определяться самой ЗС и активностью ее системой защиты [10,11].

Не менее сложной задачей, чем определение весовых коэффициентов, является задача определения вероятности нарушения ИБ различными видами угроз. Эти данные могут быть получены как опытным, так и аналитическим путем. Практически для всех угроз они будут комплексными [12]. Их можно определить с помощью выражения (2):

$$p = 1 - \prod_{j=1}^{m} (1 - p_j), \qquad (2)$$

где p_j – вероятность нарушения ИБ одной из m составляющих определенного вида угроз.

Таким образом, КП приобретает вид (3)

$$K = \sum_{i-1}^{n} (k_i (1 - (1 - \prod_{j=1}^{m} (1 - p_j)))) . \qquad (3)$$

С помощью выражения (3) можно оценить ЭИБ и сравнить между собой эффективность принимаемых решений по обеспечению ИБ в ходе проектирования и конструирования систем защиты.

Заключение

В работе рассмотрен подход к определению оценки эффективности информационной безопасности замкнутых систем. Рассмотрены возможные каналы утечки и внешнего воздействия на контуры управления замкнутых систем.

Предложенный подход позволяет формализовать оценку эффективности информационной безопасности и значительно снизить долю субъективизма путем перехода от качественных оценок к количественным.

Литература

1. Информационная безопасность. Международный стандарт безопасности ISO 17799 [Электрон. ресурс]. – Режим доступа к ресурсу: http//www.abn.ru/inf/cnews/security.shtml

2. Серков О.А. Інформаційна безпека: методи та засоби застосування / О.А. Серков, В.Я. Пєвнєв // Проблемы интеграции информации-2008 – исследования, разработки, интеллектуальная собственность: матеріали науково-практичної конференції. – Х.: НТУ «ХПІ», 2008. – С. 22.

3. Торокин А.А. Инженерно-техническая защита информации: уч. пос. для студентов, обуч. по спец. в обл. информ. безопасности / А.А.Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

4. Максименко Г.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств / Г.А. Максименко, В.А. Хорошко. – К.: ООО «ПолиграфКонсалтинг», 2004. – 317 с.

5. Кечиев Л.Н. ЭМС и информационная безопасность в системах телекоммуникаций / Л.Н. Кечиев, П.В. Степанов. – М.: Изд. дом «Технологии», 2005. – 320 с.

6. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки / Ю.К. Меньшаков. – М.: Российск. гос. гуманит. ун-т, 2002. – 399 с.

7. ДСТУ 2793-94. Сумісність технічних засобів електромагнітна. Стійкість до потужних електромагнітних завад. Загальні положення. – введ. 01.01.96. – К.:Держстандарт України, 1994. – 15 с.

8. Кравченко В.И. Электромагнитное оружие / В.И. Кравченко. – Х: НТУ «ХПИ», 2008. – 185 с.

9. Таха Х. Введение в исследование операций: в 2-х книгах. Кн.1. / Х. Таха. – М.: Мир, 1985. – 479 с.

10. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов / А.А. Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.

11. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев – К.: ООО «ТИД «ДС», 2004. – 992 с.

12. Прогнозирование ожидаемой тактики применения электромагнитного воздействия и определение перечня возможных угроз объектам управления / Е.В. Покаместов, В.В. Воскобович, И.К. Новиков, Д.А. Дегтярев // VIII Российская научно-техническая конференция по электронной совместимости и электромагнитной безопасности. ЭМС. – 2004. – С. 284-291.

Поступила в редакцию 1.02.2009

Рецензент: д-р техн. наук, проф., проф. кафедры А.А. Серков, Национальный технический университет «Харьковский политехнический институт», Харьков, Украина.

ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАМКНУТИХ СИСТЕМ

В.Я. Пєвнєв

Запропоновані визначення основних термінів, що вживаються в роботі. Аналізуються виникаючі погрози інформаційної безпеки замкнутих систем і методи їх оцінки. Розглядаються можливі критерії ефективності інформаційної безпеки. Аналізуються канали витоку інформації, характерні для закритих систем і методи протидії нав'язуванню помилкових даних. Пропонується комплексний показник визначення ефективності і спосіб його обчислення.

Ключові слова: ефективність, інформаційна безпека, критерії ефективності, показник ефективності, замкнута система, канали витоку.

EFFICIENCY OF INFORMATION SECURITY OF THE CLOSED LOOP SYSTEMS

V.Y. Pevnev

Determinations of the basic terms used in process are offered. The nascent threats to the information security of the closed loop systems and methods of their estimation are analysed. The possible efficiency criteria of information security are examined. Channels of the information leakage that are characteristic for the closed loop systems and methods to counteract the imposition of the false information are analysed. The versatility indicator of determination of the efficiency and the method of its calculation are offered.

Keywords : efficiency, information security, criteria of efficiency, versatility indicator of efficiency, closed loop system, channel leakage.

Певнев Владимир Яковлевич – канд. техн. наук, доцент, зав. кафедрой защиты информации, Харьковский национальный университет внутренних дел, Харьков, Украина.