УДК 65.012

В.Я. ПЕВНЕВ

Харьковский национальный университет внутренних дел, Украина

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАМКНУТЫХ СИСТЕМ

Предлагается формулировка понятия информационной безопасности с учетом временного фактора. Предложена классификация существующих систем по степени их открытости с точки зрения информационной безопасности. Проанализированы угрозы информационной безопасности, приведена и обоснована их классификация. Отмечена особенность классификации, представленной в работе. На основе проведенного анализа выделены и обоснованы возможные угрозы замкнутым системам.

Ключевые слова : *информационная безопасность, замкнутая система, угроза информационной безопасности, классификация систем.*

Введение

Принятая в 2009 году Доктрина информационной безопасности (ИБ) Украины [1] говорит о том, что ИБ становится важнейшей составляющей национальной безопасности. Особую актуальность ИБ приобретает в связи с использованием технических средств обработки и передачи данных при принятии решений, анализе и прогнозировании развития государства, общества и личности. Вместе с этим появляются практически не ограниченные возможности доступа к информационным ресурсам пользователей с целью противоправных действий. Это может быть незаконное получение конфиденциальной информации, которая циркулирует как в открытых, так и специальных системах, нарушение целостности информации. Оценка реальных и потенциальных угроз ИБ государства дана в [1].

Однако, задачи обеспечения ИБ возникают не только в государстве. Не менее сложные задачи этой категории появляются в системах управления предприятиями и организациями, банковских системах, локальных и корпоративных сетях, у физического лица. Для того, чтобы эффективно решать задачи обеспечения ИБ необходимо организовать построение комплексной системы защиты информации. Такая система должна иметь соответствующее правовое обеспечение, развитую организационную структуру, необходимые устройства технической защиты информации. Главная задача системы защиты - нейтрализовать возможные угрозы ИБ. При выработке технического задания на создание системы защиты необходимо проанализировать возможные угрозы ИБ. Нельзя строить систему защиты от всего, необходимо учитывать существующие реалии.

Целью работы является рассмотрение и классификация угроз ИБ замкнутых систем (ЗС).

1.Основная часть

1.1. Классификация систем

Рассмотрим определение ИБ. В [2] предложена следующая формулировка: ИБ это свойство системы противостоять несанкционированному снятию и модификации информации. В данном определении не учитывается такой фактор, как время. Поэтому предлагается следующий вариант: ИБ это свойство системы в течение заданного времени противостоять несанкционированному снятию и модификации информации. В данной работе не ставится цель расшифровки и обосновании этого определения. При желании ознакомиться с этим обоснованием, можно обратиться к работе [3]

Как видно из определения ключевым словом в нем является система. С точки зрения исследователя необходимо провести классификацию систем. В данном случае, т.к. речь идет о ИБ, следует вести разговор об открытости систем. Используя сложившуюся терминологию, следует говорить об открытых, замкнутых системах и системах с ограниченным доступом. Но такое деление является несколько упрощенным, не учитывающим переходные формы.. По мнению автора, следует ввести понятие квазиоткрытой и квазизамкнутой системы.

Под открытой системой будем понимать систему, доступ к любой части которой постоянно разрешен любому пользователю. Очевидно, что таких систем не существует. Всегда ставятся какие-то ограничения. Эти ограничения могут касаться используемой лексики, размеров сообщения, получаемых

сведений и т.д.

Под квазиоткрытой системой будем понимать такую систему, в которую ограничивается доступ по некоторым параметрам. При этом ограничения не влияют на процесс выполнения соответствующих функций в системе. Например, внесение изменений в базу данных может внести только лицо, имеющее на это полномочие, а пользователи совершенно законно используют информацию, находящуюся в ней.

ЗС будем называть такую систему, в которой все элементы, включая оконечные устройства и составляющие каналов связи, находятся на охраняемой территории. В ЗС невозможно внести какую-либо информацию, произвести ее искажение либо снятие. Реально таких систем не существует. Любую систему можно уничтожить, тем самым уничтожить информацию, находящуюся в ней.

Под квазизамкнутой системой будем понимать такую систему, в которой минимизируется доступ к информации по большинству параметров, а по возможности, закрывается вообще.

Системы с ограниченным доступом занимают промежуточное место в классификации систем между квазиоткрытыми и квазизамкнутыми системами. По своим характеристикам и эксплутационным возможностям они ближе к квазиоткрытым системам.

В дальнейшем, при изложении материала под термином ЗС будем понимать квазизамкнутую систему.

1.2. Классификация угроз

Прежде чем приступить к классификации угроз для ИБ ЗС, следует отметить, что в предлагаемой работе не рассматриваются угрозы, связанные с человеческим фактором.

Под угрозой, согласно [4] понимается утечка, возможность блокирования или нарушения целостности информации. Более точная, по мнению автора, формулировка угрозы содержится в [5]: совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. В данном контексте термины ИБ и безопасность информации совпадают.

Проведем классификацию основных видов угроз ИБ. По мнению автора, следует выделить несколько классов угроз:

- по типу угроз;
- по месту расположения источника угроз;
- по воздействию на информацию,
- по типу доступа к информации;
- по времени воздействия на информацию.

Рассмотрим перечисленные угрозы. В первую очередь необходимо определить тип угроз. Очевидно, что такие угрозы следует разделить на :

- естественные угрозы;
- искусственные угрозы.

К естественным угрозам относятся такие, которые носят природный характер. Это ураганы, землетрясения, грозы и т. д. К данному типу угроз можно отнести и пожары, но с оговоркой, что они возникли не по вине человека.

Искусственные угрозы возникают в результате человеческой деятельности. К их возникновению приводит как целенаправленные противоправные действия, так и обычная невнимательность, нарушения правил обращения с оборудованием, приборами, носителями информации.

Рассмотрим угрозы по месту расположения их источника. В этом случае можно говорить о:

- внешней угрозе;
- внутренней угрозе;
- внесенной угрозе.

Под внешней угрозой будем понимать те угрозы, которые возникают за пределами периметра ЗС. К данному типу угроз можно отнести, например, возможность снятия информации с помощью побочного электромагнитного излучения или перехват сообщений при их передачи по линиям связи (телефонным, воздушным, оптоволоконным и т.д.).

Внутренние угрозы возникают внутри периметра ЗС. Чаще всего это дефекты объектов и аппаратуры, нарушения правил и мер безопасности, правил эксплуатации, которые могут привести к утечки, искажению или к уничтожению информации.

Самыми опасными являются внесенные угрозы. Под такими угрозами следует понимать заранее внесенные дефекты оборудования, сооружений, технических систем и программных продуктов, которые не были выявлены в процессе испытаний и эксплуатации, неточности в эксплуатационной документации, а также законсервированные в строительные конструкции или доставленные в сувенирах и подарках устройства снятия информации.

Следующим признаком, по которому следует провести классификацию угроз, следует считать результат воздействия на информацию. Здесь можно выделить следующие угрозы:

- несанкционированное снятие;
- искажение (вплоть до уничтожения);
- отказ;
- навязывание.

Под несанкционированным снятием понимается использование технических и других средств для получения информации. При этом возможно как

подключение к носителям информации, так и использование побочных факторов. К этому виду угроз можно отнести прослушивание телефонных линий, прием паразитных электромагнитных излучений, скрытая фото- и видеосъемка.

Под искажением следует отнести действия, направленные на нарушение целостности информации. Данная угроза, пожалуй, единственная, которая может возникать независимо от человека.

Под отказом следует понимать отрицание подлинной информации. Данная угроза может быть исполнена как по причине наличия ошибок в эксплуатационной документации, так и причине дефектов.

Под навязыванием следует понимать информацию, принятую к исполнению, которая была получена либо от фиктивного лица, либо отправленная от имени известного лица, но сфальсифицирована нарушителем. Другими словами данная угроза предполагает принятие ложной информации за истинную.

Одной из самых серьезных угроз является угроза по типу доступа к информации. При этом следует выделить:

- несанкционированный доступ;
- блокирование доступа.

Под несанкционированным доступом (НСД) понимается незаконное проникновение в закрытое информационное пространство. Согласно [4] НСД это доступ к информации, при котором нарушаются порядок его осуществления и установленные правовые нормы. В качестве примера можно рассмотреть доступ к закрытым базам данных силовых ведомств или банковских структур.

Под блокировкой понимается такое состояние системы, которое не позволяет осуществить законный доступ ко всей информации, циркулирующей в этой системе, или какой-либо ее части. Такую блокировку можно осуществить, например, с помощью хакерской атаки, когда на сервер за короткое время приходит такое количество запросов, которое невозможно обслужить.

Следующим пунктом следует выделить распределение угроз по времени воздействия:

- мгновенное;
- длительное;
- отсроченное.

В качестве примера мгновенной угрозы можно показать действие электромагнитного импульса на элементы памяти. Угрозы длительного действия позволяют накапливать или разрушать информацию за какой-то, достаточно большой, промежуток времени.

Отсроченной угрозой будем называть такие угрозы, которые начинают действовать либо в заранее назначенное время, либо по истечении определенного срока. В качестве примера можно показать угрозу уничтожения информации с помощью пожара, если при строительстве был проложен электрический провод меньшего диаметра.

1.3. Угрозы в замкнутой системе

При рассмотрении угроз ИБ ЗС будем рассматривать те угрозы, которые были представлены в предыдущем параграфе. Исходя из определения, данного ЗС, можно говорить о том, что в качестве угроз отсутствует угроза по типу доступа.

Если рассматривать угрозы по типу, по месту расположения источника угроз, по воздействию на информацию, по времени воздействия на информацию, то они остаются такими же, за исключением навязывания. Следует лишь остановиться на особенностях этих угроз в ЗС.

При конструировании ЗС учитываются возможные природные явления. Например, подобную систему не расположат в зоне возможного затопления, будет спроектирована эффективная защита от удара молнии. Т.е. рассмотрение природных угроз ЗС осуществляется на этапе создания систем.

Особенностью несанкционированного снятия информации является возможность производить его лишь дистанционно, при этом исключается возможность использования телефонных линий связи, различного рода закладных устройств. Основным источником получения информации является побочное электромагнитное излучение.

Угроза искажения возникает при дистанционном воздействии на информацию, поступающей с различных датчиков или направляемой к исполнительным устройствам, с целью ее модификации. Данную угрозу можно осуществить ЭМИ узкого частотного диапазона.

С помощью мощного ЭМИ можно оказать поражающее воздействие как на элементы конструкции [6], так и на элементную базу информационной системы, даже если она находится в выключенном состоянии [7]. Данное воздействие может привести к физическому уничтожению информационной системы.

Заключение

В работе предложена формулировка понятия ИБ с учетом временного фактора. Проведена классификация существующих систем с точки зрения ИБ. Автором предложена и обоснована классификация угроз ИБ по различным признакам. Следует отметить особенность классификации, представленной в работе. Когда происходит переход к конкретным

угрозам, то оказывается , что они принадлежат различным типам угроз. Например, угроза несанкционированного снятия может осуществляться как внешняя, внутренняя или внесенная угроза.

На основе проведенного анализа выделены и обоснованы угрозы ИБ ЗС.

Литература

1. *Доктрина інформаційної безпеки України [Электрон.ресурс]. – Режим доступа к ресурсу: http//www. President. qov. ua/ documents/9570.*

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 НПК. – Х.: НТУ «ХПІ», 2008. – С. 22.

3. Певнев В.Я. Эффективность информационной безопасности замкнутых систем / В.Я. Певнев // Радіоелектронні і компютерні системи. – 2009. – № 5(37). – С. 82–85.

4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. введ.01.01.98. – К.: Держстандарт України, 1997. –16 с.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.введ. 02.01.08. – М.: Стандартинформ, 2008. – 8 с.

6. Космическое оружие: дилемма безопасности / под ред. Е.П.Велихова, Р.З. Сагдеева, А.А. Кокошкина. – М., Мир, 1986. –182 с.

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

Поступила в редакцию 9.02.2010

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

АНАЛИЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАМКНЕНИХ СИСТЕМ

В.Я. Пєвнєв

Запропоновано визначення терміну інформаційна безпека з урахуванням часового фактору. Запропонована класифікація існуючих систем за степеню їх відвертості з точки зору інформаційної безпеки. Проаналізовані загрози інформаційної безпеки, наведена та обґрунтована їх класифікація. Відзначена особливість класифікації, наведеної у роботі. На основі проведеного аналізу визначені та обґрунтовані можливі загрози системам, що замкнути.

Ключові слова: інформаційна безпека, замкнута система, загроза інформаційної безпеки, класифікація систем

THE ANALYSIS OF THREAT OF INFORMATION SECURITY OF THE CLOSED LOOP SYSTEMS

V.Y. Pevnev

The formulation of concept of information security taking into account the time factor is offered. Classification of existed systems by degree of their openness from the point of view of information security is offered. Threats of information security are analyzed, and their classification is spent and grounded. Classification feature that was marked out in the work is presented. O the base of taken analysis possible threats to the closed loop systems are singled out and proved.

Key words : information security, closed loop system, threat of information security, classification of systems.

Певнев Владимир Яковлевич, канд. техн. наук, доцент, зав. кафедрой защиты информации Харьковского национального университета внутренних дел, Харьков, Украина.