

УДК 65.012:34(477)

В.Я. Певнев, М.В. Цуранов

Харьковский национальный университет внутренних дел, Харьков

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются существующие определения информационной безопасности, показываются недостатки этих определений. Предлагается определение информационной безопасности, которое основывается на системном подходе. Рассматриваются функции информационной безопасности с точки зрения свойств информации и средства ее обеспечения. Представлена математическая модель информационной безопасности.

Ключевые слова: информация, информационная безопасность, целостность информации, модификация.

Введение

Постановка проблемы. Согласно Доктрине информационной безопасности Украины [1] обеспечение ИБ относится к наиболее важным функциям государства. Это положение показывает место ИБ в безопасности всего государства. В [1] также определены жизненно важные интересы в информационной среде личности, общества и государства которые нуждаются в защите со стороны государства. Вместе с тем в существующих законах нет понятия ИБ. Более того, оно отсутствует и в универсальной десятичной классификации [2]. Другими словами, ИБ как бы не существует.

Анализ литературы. Несмотря на перечисленные сложности, существует большое количество определений, которые отражают то или иное представление ИБ. Рассмотрим некоторые из них.

В работе [3] представлено следующее определение ИБ (цитирую языком оригинала): «інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави». Данное толкование ставит знак равенства между ИБ и ИБ государства, т.е. сужает само понятие ИБ. В настоящее время нет закона, который бы определял ИБ, соответственно нет правил по которым происходит информационный процесс с точки зрения ИБ.

В работе [4] говорится, что «інформаційна безпека – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від внутрішніх і зовнішніх інформаційних загроз». Это определение созвучно с понятием ИБ, которое положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации: «ИБ – это состояние защищен-

ности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз» [5]. Данное определение также не отражает сущности ИБ, сужая его только до общественных взаимоотношений.

Во многих работах и выступлениях происходит подмена понятия ИБ на безопасную информацию или безопасность информации. Это видно на примере материалов круглого стола «Информационная безопасность Украины: сущность и проблемы», проведенного в июне 1998 г. [6]. На взгляд авторов, такой подход неправилен, т.к. уводит читателя от сущности ИБ. Определение ИБ не должно зависеть от того, о каком предмете идет речь. ИБ одна, и, давая определение, нужно исходить из этого.

Цель статьи – обосновать определение ИБ и ее математической модели.

Изложение основного материала

Определение ИБ. Исторически понятие ИБ появилось как калька английского термина information security. Равнозначным его переводом является и защита информации.

Следует рассмотреть те особенности ИБ, основываясь на которые можно дать определение этому термину. Когда говорят об ИБ, то речь должна идти о какой-либо системе, быть то государство, корпорация, телекоммуникационная сеть или что-то другое.

Согласно [7], под системой понимается объединение некоторого разнообразия в единое и четко расчлененное целое, элементы которого по отношению к целому и др. частям занимают соответствующие им места.

Каждая система обладает рядом свойств и может находиться в том или ином состоянии. По аналогии с надежностью [8], говоря об ИБ надо говорить не о состоянии, а о свойстве системы. Таким образом, можно сказать, что ИБ – это свойство системы.

Понятие ИБ всегда должно быть логически привязано к информации, средствам ее обработки, хранения, доставки, воздействия на объект. В жизненном цикле информация может быть подвергнута различного вида воздействиям, которые направлены на нарушения конфиденциальности, целостности и доступа к информации [9].

Следует сказать что во многих нормативных документах как ИБ так и ИБ государства рассматриваются в данный конкретный момент времени, например в [1] говорится, что «Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду».

Исходя из вышеизложенного, авторами предлагается следующее определение ИБ: **информационная безопасность – свойство системы в течении заданного времени противостоять несанкционированному снятию и модификации информации.**

Под несанкционированным снятием понимается получение информации, к которой у абонента нет доступа, т.е. нарушение правил 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.

Функции ИБ. Исходя из представленного определения, можно рассмотреть составляющие ИБ. В первую очередь необходимо говорить о конфиденциальности информации. Согласно [10], «конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов». Основываясь на положение Закона, ставиться задача на ограничение доступа к тому или иному виду информации. При решении этой задачи можно говорить о двух направлениях: первое – работа с законопослушными пользователями информации, которые выполняют все инструкции по организации допуска, и второе – когда речь идет о преднамеренном снятии закрытой информации. В этом случае необходимо проводить ряд организационных и технических мероприятий по защите информации.

Таким образом, можно определить первую функцию ИБ – это организация работ по ограничению доступа к информации.

Особое значение придается целостности информации. Большинство исследователей не привязывает целостность к конкретной системе, и идентифицируют ее с цифровой подписью.

На взгляд авторов система должна обеспечить проверку целостности информации. Обеспечение

целостности требует огромного числа правовых, организационных и технических мероприятий, позволяющих предотвратить нарушение целостности информации и реализовать это требование на современном этапе развития практически не возможно.

Исходя из сказанного выше, можно сформулировать вторую функцию ИБ – контроля и, по возможности, обеспечения целостности информации.

Говоря о следующей составляющей ИБ – доступности, то опосредствовано она описана в конфиденциальности, т.е. ограничении (разграничении) доступа.

Если информация не является закрытой, то она должна быть доступной для всех. Причем информация должна быть доступна в любой момент времени. В этом случае возникает проблема организации свободного доступа к официально доступной информации. Однако, достаточно часто, путем блокирования как организационными, так и техническими способами производится ограничения доступа к той или иной информации.

Более подробно функции ИБ рассмотрены в [11].

Математическая модель ИБ. Исходя из функций ИБ, ее можно представить в виде:

$$\sum_i^n f(C_i, I_i, A_i) \Rightarrow \max \quad (1)$$

при $f(C_i, I_i, A_i) > D_{зад_i}$,

где $f(C_i, I_i, A_i)$ – значение функции ИБ для i -ой угрозы; n – количество угроз; C_i, I_i, A_i – вероятность нарушения целостности, доступности и конфиденциальности для i -й угрозы; $D_{зад_i}$ – заданный уровень ИБ i -й угрозы.

Исходя из данного в статье определения ИБ формула (1) примет следующий вид:

$$\sum_i^n f(C(\Delta t)_i, I(\Delta t)_i, A(\Delta t)_i) \Rightarrow \max ; \quad (2)$$

при $\Delta t > t_{зад}$; $\Delta t = t_{кв} - t_{ну}$,

где Δt – время в течении которого реализуется i -я угроза целостности, доступности или конфиденциальности ИБ; $t_{зад}$ – время в течении которого необходимо поддерживать заданный уровень ИБ.

Для количественного оценивания выражений (1) и (2) предлагается использовать метод, изложенный в [12], с помощью которого можно определить комплексный показатель эффективности ИБ системы.

Средства обеспечения ИБ. Для обеспечения ИБ необходимо применять юридические и морально-этические нормы (МЭН), технические средства защиты информации (ТСЗИ).

Говоря о юридических нормах, следует отметить отсутствие в стране закона об ИБ. Такой закон мог бы позволить провести изменения в другие законы и кодексы, например, обязать руководителей предприятий заниматься вопросами ИБ на стадии разработки проекта, а не после утечки информации.

Необходимо отметить одну особенность использования МЭН при обеспечении ИБ различных систем. Если нами будет поднят вопрос об обеспечении ИБ государства, то МЭН, а точнее соблюдение этих норм, политической элиты выходят на первый план. При обеспечении ИБ предприятия МЭН необходимо учитывать при наборе сотрудников.

В обеспечении ИБ наиболее важная роль принадлежит ТСЗИ. Нарушитель не остановится ни перед законом, ни перед МЭН. Единственное, что его может остановить – это ТСЗИ.

Под ТСЗИ понимаются устройство и (или) программное средство, в которых функция защиты информации является основной [13]. В современном мире это большой арсенал средств противодействия любителям незаконного снятия информации.

Выводы

Представленное в работе определение ИБ отражает сущность этого термина, не привязываясь к конкретной системе. Главным отличием от предложенных ранее определений является введение временной составляющей. Рассмотрены основные функции систем ИБ, основываясь на которых, сформулирована математическая модель.

Список литературы

1. Доктрина інформаційної безпеки України. ЗАТВЕРДЖЕНО Указом Президента України від 8 липня 2009 року № 514/2009 [Электронный ресурс]. – Режим доступа к док.: <http://www.president.gov.ua/documents/9570.html>.
2. Універсальна десяткова класифікація: У 2 кн. / Голвн. ред. М.І. Сенченко; UDC Consortium, Кн. палата України. – К.: Кн. палата України, 2000. – 932 с.

3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібник / Б.А. Кормич. – К.: Кондор, 2004. – 384 с.
4. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдин. – К.: МК-Прес, 2005. – 432 с.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебн. пособие для вузов / А.А. Малюк. – М.: Горячая линия-Телеком, 2004. – 280 с.
6. Інформаційна безпека України: сутність та проблеми. Матеріали круглого столу. [Електронний ресурс]. – Режим доступу к документу: www.nirr.gov.ua/ukr/publishing/panorama3_4.
7. Философский энциклопедический словарь. – М.: ИНФРА-М, 2000. – 576 с.
8. Новый энциклопедический словарь. – М.: Большая Российская энциклопедия, РИПОЛ Классик, 2004. – 1456 с.
9. Гринберг А.С. Защита информационных ресурсов государственного управления: учебн. пособие для вузов / А.С. Гринберг, Н.Н. Горбачев, А.А. Тепляков. – М.: ЮНИТИ-ДАНА, 2003. – 327 с.
10. Закон України «Про інформацію» // Відомості Верховної Ради. – 1992. – № 48.
11. Серков О.А. Информационная безопасность: концепция и средства обеспечения / О.А. Серков, В.Я. Певнев // Вестник национального технического университета «ХПИ». – Х., 2008. – № 44. – С. 132-136.
12. Певнев В.Я. Эффективность информационной безопасности замкнутых систем / В.Я. Певнев // Радіоелектронні і комп'ютерні системи. – 2009. – № 5. – С. 82-85.
13. ДСТУ 3396.2-97. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Держстандарт України, 1997. – 20 с.

Поступила в редколлегию 25.03.2010

Рецензент: д-р техн. наук, доцент А.В. Потий, Харьковский университет Воздушных сил им. И. Кожедува, Харьков.

МАТЕМАТИЧНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В.Я. Певнев, М.В. Цуранов

Розглядаються існуючі визначення інформаційної безпеки, показуються недоліки цих визначень. Пропонується визначення інформаційної безпеки, що ґрунтується на системному підході. Розглядаються функції інформаційної безпеки з точки зору властивостей інформації та засоби її забезпечення. Представлено математичну модель інформаційної безпеки.

Ключові слова: інформація, інформаційна безпека, цілісність інформації, модифікація.

MATHEMATICAL MODEL OF INFORMATION SECURITY

V. Ya. Pevnev, M. V. Tsuranov

We consider the existing definitions of information security, the shortcomings of these definitions. Proposed definition of information security, which is based on a systemic approach. We consider the function of information security in terms of properties of information and means to ensure it. Submitted a mathematical model of information security.

Key words: information, information security, information integrity, modification.