УДК 681.3

Доцент Е.В. Белокурова, доцент А.А. Дерканосова
(Воронежский государственный университет инженерных технологий)
кафедра сервиса и ресторанного бизнеса, тел. (473) 2553-882
адъюнкт А.А. Змеев
(Воронеж, ВИ ФСИН России) кафедра МиЕНД. тел. (8473)260-68-19
аспирант А.П. Сидельников
(Воронеж, ВГТУ) кафедра СИБ. тел. (8473)274-57-14

Associate Professor E.V. Belokurova,
associate Professor A.A. Derkanosova
(Voronezh state university of engineering technology)
Department of service and restaurant business. phone (473) 2553-882
associate A.A. Zmeev
(Voronezh Institute of the Federal Penitentiary Service)
Department of mathematics and natural sciences. phone (8473) 260-68-19
graduate A.P. Sidelnikov
(Voronezh, Voronezh State Technical University) Department of NIB. phone (8473) 274-57-14

Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем

Methods for assessing security threats confidential information for the Information and telecommunications systems

Реферат. В статье рассматривается различные подходы к оценке безопасности конфиденциальной информации для информационно-телекоммуникационных систем различно предметного назначения в условиях наличия внутренних и внешних угроз ее целостности и доступности. Сложности с обеспечением безопасности конфиденциальной информации от воздействия на информационно-телекоммуникационную системы внешних и внутренних угроз в настоящее время приобретает особую актуальность. Указанная проблема подтверждается анализом имеющейся статистической информации о влиянии угроз на безопасность, циркулирующей в информационно-телекоммуникационной системе. Утечка конфиденциальной информации, интеллектуальной собственности, информации «ноу-хау» является следствием значительного материального и морального ущерба, который наносится собственнику информации ограниченного распространения. В работе приведена структура показателей и критериев свидетельствует о том, что наиболее перспективными являются аналитические критерии. Однако их применение для оценки уровня безопасности конфиденциальной информации затруднительно из-за отсутствия соответствующих математических моделей. Сложность проблемы заключается в том, что традиционные существующие математические модели не всегда приемлемы для указанных целей. Следовательно, необходима разработка математических моделей, предназначенных для оценки безопасности конфиденциальной информации с учетом воздействия на информационно-телекоммуникационную систему угроз.

Summary. The article discusses the different approaches to assessing the safety of confidential information-term for information and telecommunication systems of various pre-appreciable destination in the presence of internal and external threats to its integrity and availability. The difficulty of ensuring the security of confidential information from exposure to information and telecommunication systems of external and internal threats at the present time, is of particular relevance. This problem is confirmed by the analysis of available statistical information on the impact of threats on the security circulating in the information and telecommunications system. Leak confidential information, intellectual property, information, know-how is the result of significant material and moral damage caused to the owner of the restricted information. The paper presents the structure of the indicators and criteria shows that the most promising are analytical criteria. However, their use to assess the level of security of confidential information is difficult due to the lack of appropriate mathematical models. The complexity of the problem is that existing traditional mathematical models are not always appropriate for the stated objectives. Therefore, it is necessary to develop mathematical models designed to assess the security of confidential information and its impact on information and telecommunication system threats.

Ключевые слова: защита информации, угроза, информационная система.

Keywords: information security, threat, information system.

Проблема, связанная с обеспечением безопасности конфиденциальной информации (КИ) от воздействия на информационно-телекоммуникационную системы (ИТКС) внешних и внутренних угроз в настоящее время приобретает особую актуальность. Указанная проблема подтверждается анализом имеющейся статистической информации о влиянии угроз на безопасность КИ, циркулирующей в ИТКС. Утечка КИ, интеллектуальной собственности, информации «ноу-хау» является следствием значительного материального и морального ущерба, который наносится собственнику информации ограниченного распространения.

Хаотичный и в ряде случаев неконтролируемый рост числа абонентов сети, увеличение объемов хранимой и передаваемой информации, территориальная разнесённость сетей приводят к возрастанию потенциально возможного количества преднамеренных и непреднамеренных нарушений безопасности информации, возможных каналов или уязвимых звеньев несанкционированного проникновения в сети с целью чтения, копирования, подделки программного обеспечения, текстовой и другой информации.

Под угрозой информационной безопасности (ИБ) понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы ИБ в ИТКС направлены на нарушение функционирования следующих компонентов ИТКС [1]:

- компьютеров с сетевыми адаптерами;
- коммуникационных элементов самого различного назначения;
- средства приема и передачи данных;
- средства отображения и хранения информации;
- технические системы и средства защиты информации;
- помещения, где располагается большинство узлов ИТКС.

При построении обобщенной модели угроз информационной безопасности ИТКС следует подробно рассмотреть следующие вопросы:

- классификацию угроз безопасности информации;
- определение видов представления информации, подлежащей защите в ИТКС и определение возможных каналов ее утечки;
- создание модели вероятного злоумышленника.

Угрозы информационной безопасности по степени преднамеренности можно разделить на:

- случайные, т.е. источником могут быть ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей или администрации сети и т.п.;
- умышленные угрозы в отличие от случайных преследуют цель нанесения ущерба пользователям сети и, в свою очередь, подразделяются на активные и пассивные;
- пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование сети;
- активные угрозы имеют целью нарушить нормальный процесс функционирования сети посредством целенаправленного воздействия на ее аппаратные, программные и информационные ресурсы. Источниками таких угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

В зависимости от местонахождения источника возможной угрозы все угрозы делятся на две группы: внешние и внутренние. К внешним угрозам информационной безопасности (ИБ) относятся:

- деятельность иностранных разведывательных и специальных служб;
- деятельность конкурирующих иностранных экономических структур;
- деятельность политических и экономических структур, преступных групп и формирований, а также отдельных лиц внутри страны, направленная против интересов граждан, государства и общества в целом и проявляющаяся в виде воздействий на ИТКС;
- стихийные бедствия и катастрофы.

К внутренним угрозам ИБ относятся:

- нарушения установленных требований ИБ (непреднамеренные либо преднамеренные), допускаемые обслуживающим персоналом и пользователями ИТКС;
- отказы и неисправности технических средств обработки, хранения и передачи сообщений (данных), средств защиты и средств контроля эффективности, принятых мер по защите;
- сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности принятия мер по защите.

Сложность и комплексность проблемы анализа и синтеза информационно-телекоммуникационных систем, иерархичность построения, присущая таким системам, предполагает, что оценка безопасности конфи-

денциальной информации должна осуществляться с применением системы показателей и критериев. Результаты такой оценки являются основой для принятия решений из некоторого множества альтернатив. Исследования показывают, что в указанных целях наиболее перспективным является применение статистических показателей и вероятностных критериев.

Статистические показатели могут быть абсолютными и относительными. В то же время абсолютные и относительные статистические показатели подразделяются на общие и частные.

Общие показатели характеризуют безопасность КИ по всем факторам или причинам, приводящим к угрозам, а частные — по конкретным факторам и причинам или по группам причин.

К общим абсолютным статистическим показателям безопасности КИ можно отнести следующие [1]:

- общее число угроз, воздействующих на ИТКС за определенный период (сутки, месяц, год и т. п.) n_y;

- абсолютный ущерб, нанесенный собственнику в результате воздействия на ИТКС внутренних угроз (например, тыс. рублей) $R_{ущ}$.

Абсолютные статистические показатели могут применяться для:

- выявления общих тенденций в динамике угроз, воздействующих на ИТКС;

- выявления и прогноза общего ущерба от воздействия угроз на ИТКС;

- разработки и применения плановых профилактических мероприятий по предупреждению появления угроз, их локализации и снижения величины ущерба от их реализации.

Основным недостатком абсолютных статистических показателей является то, что они характеризуют уровень безопасности КИ за прошедший период и не позволяют осуществлять прогноз на ближайшую перспективу.

К общим относительным статистическим показателям безопасности КИ относятся [1]:

- средняя наработка ИТКС на одну внутреннюю угрозу за определенный период (например, за год)

$$T_{ср} = \frac{t_\Sigma}{n_y}, \qquad (1)$$

где t_Σ - суммарная наработка ИТКС за определенный период; n_y - количество внутренних угроз, проявившихся за этот же период;

- средняя наработка ИТКС на одну внутреннюю угрозу с последствиями за определенный период (например, за год):

$$T_{ср} = \frac{t_\Sigma}{(n_y)_{пос}}, \qquad (2)$$

где $(n_y)_{пос}$ — количество угроз с последствиями за определенный период;

- средняя величина ущерба на одну угрозу с последствиями:

$$\overline{R} = \frac{R_\Sigma}{(n_y)_{пос}}, \qquad (3)$$

где R_Σ - суммарная величина ущерба собственнику за определенный период (например, за год).

Общие относительные показатели безопасности КИ позволяют оценить общую тенденцию изменения наработки и наработки с последствиями с учетом воздействия на ИТКС внутренних угроз. При этом следует отметить, что вследствие применения замкнутых механизмов, совершенствования политики безопасности, проведения организационно-профилактических мероприятий, данные показатели имеют устойчивую тенденцию повышения.

В целом, общие статистические показатели имеют интегральный характер и не позволяют осуществить оценку и прогнозирование по отдельным угрозам, особенно тем, которые приводят к существенным последствиям. Эту задачу можно решить с помощью частных статистических показателей.

К частным статистическим показателям относятся [1]:

- распределение внутренних угроз по причинам, вызвавшим их появление (халатность, безответственность и т. п. сотрудников организации);

- распределение внутренних угроз по последствиям от воздействия на ИТКС (например, кража, подмена, уничтожение КИ и т. п.);

- распределение внутренних угроз по частоте появления однотипных внутренних угроз (например, частота кражи, подмены, перехвата КИ и т. п.);

- распределение внутренних угроз по степени риска собственнику КИ (например, наибольший, повышенный, средний, ограниченный, низкий и т. п.);

- распределение внутренних угроз по последствиям от воздействия внутренних угроз на КИ (например, катастрофические, критические, существенные, малосущественные, несущественные последствия).

Использование частных статистических показателей позволяет определить уровень безопасности КИ по отдельным внутренним угрозам, причинам их вызвавшим, последствиям воздействия на ИТКС в целом и ее элементы.

Использование информации, полученной в процессе принятия частных статистических показателей для анализа состояния безопасности КИ, предполагает разработку и проведение научно-обоснованных мероприятий по предупреждению или полной ликвидации наиболее опасных внутренних угроз за счет проведения целевой профилактической работы среди сотрудников, допущенных к работе с КИ и пользователей КИ. Однако статистические показатели обладают существенными недостатками. Они заключаются в следующем [2]:

- такие показатели оценивают безопасность КИ за прошедший период;

- по таким показателям не представляется возможным осуществлять прогнозирование безопасности КИ.

Указанные недостатки возможно парировать за счет принятия для оценки безопасности КИ вероятностных критериев.

Воздействие внутренних угроз на элементы системы ИТКС в общем виде носит случайный характер и может привести к двум исходам [2]:

- благополучный исход в случае, если цель воздействия внутренних угроз на ИТКС не достигнута;

- неблагополучный исход во всех остальных случаях.

В связи с этим в качестве критерия оценки безопасности КИ можно принять вероятность благополучного исхода при воздействии на ИТКС внутренних угроз [3].

Обозначим указанную вероятность через p. Вероятность противоположного события, т. е. вероятность неблагополучного исхода при воздействии на ИТКС внутренних угроз, будет равна q. Указанные события составляют полную группу независимых событий.

Тогда:

$$p + q = 1 \qquad (4)$$

Нетрудно заметить, что вероятности p и q являются аналитическими критериями оценки безопасности КИ.

Как уже было отмечено, на безопасность КИ оказывают влияние многочисленные факторы [3]. Поэтому для оценки безопасности КИ могут применяться различные подходы. Однако, как показывает анализ [3], для такой оценки необходимо учитывать тот факт, что в результате воздействия на ИТКС внутренних угроз она может перейти из исходного (нормального) состояния в другое, особое, состояние, соответствующее возникновению особой ситуации. В то же время появление особых ситуаций связано с угрозой безопасности КИ, циркулирующей в ИТКС.

Переход ИТКС из одного состояния в другое является следствием вполне конкретных причин. Однако возникают они, как правило, в произвольный момент времени, поэтому их появление случайно. Каждая особая ситуация может привести как к благополучному, так и неблагополучному исходу для КИ с учетом успешности (не успешности) действий сотрудников по парированию последствий появления особых ситуаций.

Обозначим вероятность возникновения i-й особой ситуации через q_i, условную вероятность парирования ее последствий через r_i, а вероятность непарирования — через $\overline{r_i}$.

Тогда для определения вероятностей p_i и q_i, представим последовательность переходов ИТКС от одного (исходного) состояния к другому марковским случайным процессом со счетным множеством состояний и непрерывным временем.

Такое представление обусловлено следующими допущениями:

- в исходном состоянии ИТКС находится в нормальном состоянии;

- последовательность возникновения особых ситуаций i-го вида является простейшим потоком с интенсивностью λ_i;

- интенсивность благополучного исхода обозначена через $\lambda_i r_i$, а неблагополучного - $\lambda_i \overline{r_i}$

Сущность метода расчета вероятностей p_i и q_i при использовании марковского процесса состоит в том, что неизвестные вероятности определяются из решения дифференциальных уравнений, которые описывают этот процесс. Анализ показывает, что такой процесс целесообразно представить в виде логико-вероятностного процесса [3].

Предположим, что возможные состояния ИТКС в процессе воздействия на нее угроз определены. Кроме того, известны направления ее случайных переходов из состояния в состояние.

Тогда вполне возможно построить логическую схему (граф) состояния, которая при известных вероятностях перехода системы из состояния в состояние представляет собой логико-вероятностную модель ИТКС (рисунок 1, по аналогии с [3]).

На рисунке 1 представлена логическая схема воздействия на ИТКС одной i -й угрозы.

Правомочность такого представления ИТКС основана на том, что возможные исходы от воздействия на ИТКС являются случайными событиями в силу случайности появления тех или иных внутренних угроз.

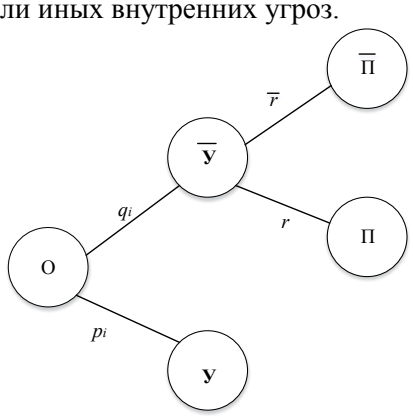

Рисунок 1. Логико-вероятностный процесс воздействия на ИТКС i -й внутренней угрозы

В соответствии с рисунком 1 следует, что в процессе функционирования ИТКС существует некоторая опасность, связанная с воздействием на нее i -й угрозы. При таком воздействии ИТКС может находиться в следующих состояниях (рисунок 1):

- «О» - начальное состояние ИТКС;
- «$У$»- состояние, когда i-я внутренняя угроза не проявляется с вероятностью p_i
- «$\overline{У}$» - состояние, когда i-я внутренняя угроза проявилась с вероятностью:

$$q_i = 1 - p_i \quad (5)$$

- «$П$» — состояние парирования внутренней угрозы с вероятностью r;
- «$\overline{П}$» — состояние не парирования последствий проявления внутренней угрозы с вероятностью $\bar{r} = 1 - r$.

Конечные состояния «$\overline{У}$» и «П» соответствуют благополучному исходу при воздействии на ИТКС i -й угрозы.

Состояние «$\overline{П}$» соответствует неблагополучному исходу при воздействии на ИТКС i -й внутренней угрозы. Тогда, в соответствии с рисунком 1, вероятность благополучного исхода от воздействия на ИТКС i-й угрозы определяется следующим образом:

$$P_{бu_i} = p_i + q_i * r_i \quad (6)$$

а вероятность неблагополучного исхода:

$$Q_{бu_i} = q_i * \bar{r}_i \quad (7)$$

Так как вероятности $P_{бu_i}$ и $Q_{бu_i}$ составляют полную группу событий, то:

$$P_{бu_i} + Q_{бu_i} = 1 \quad (8)$$

Из (8) следует, что:

$$P_{бu_i} = 1 - Q_{бu_i} \quad (9)$$

$$Q_{бu_i} = 1 - P_{бu_i}$$

Таким образом, с точки зрения последствий воздействия на ИТКС внутренней угрозы на основе анализа выражений (8) можно сделать нижеследующие выводы.

1. Количественной мерой, характеризующей последствия от воздействия i -й внутренней угрозы на КИ, являются вероятность благополучного исхода $P_{бu_i}$ и вероятность противоположного события, т. е. вероятность неблагополучного исхода в результате воздействия i-й внутренней угрозы на ИТКС, т. е. $Q_{бu_i}$.

2. Анализ выражения (8) свидетельствует о том, что вероятности $P_{бu_i}$ и $Q_{бu_i}$ являются критериями количественной оценки последствий от воздействия на ИТКС i-й внутренней угрозы.

3. Анализ выражения (8) также показывает, что для количественной оценки последствий воздействия внутренних угроз на ИТКС достаточно определить любую составляющую, например $Q_{бu_i}$. Определение другой составляющей из выражения (8) не представляет сложностей.

Таким образом, в статье приведенная структура показателей и критериев свидетельствует о том, что наиболее перспективными являются аналитические критерии. Однако их применение для оценки уровня безопасности КИ затруднительно из-за отсутствия соответствующих математических моделей.

Сложность проблемы заключается в том, что традиционные существующие математические модели не всегда приемлемы для указанных целей. Следовательно, необходима разработка математических моделей, предназначенных для оценки безопасности КИ с учетом воздействия на ИТКС угроз.

ЛИТЕРАТУРА

1 Минаев В.А., Скрыль С.В. Основы информационной безопасности: учебник для высших учебных заведений МВД России. Воронеж: Воронежский институт МВД России, 2001. 464 с.

2 Белокуров С.В., Скрыль С.В., Джоган В.К. и др. Методы и средства анализа эффективности систем информационной безопасности при их разработке: монография. Воронеж: Воронежский институт МВД России, 2012. 83 с.

3 Белокуров С.В., Скрыль С.В., Джоган В.К. и др. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах: монография. Воронеж: Воронежский институт МВД России, 2012. 116 с.

REFERENCES

1 Minaev V.A., Skryl' S.V. Osnovy informatsionnoi bezopasnosti [Foundations: the textbook for higher educational institutions Ministry of Interior of Russia]. Voronezh, Voronezh Institute of the Ministry of Interior, 2001. 464 p. (In Russ.).

2 Belokurov S.V., Skryl' S.V., Joghan V.K. et al. Metody i sredstva analiza effektivnosti system informatsionnoi beopasnosti pri ikh razrabotke [Methods and tools for analyzing the effectiveness of information security in their development: a monograph]. Voronezh Voronezh Institute of Russian Ministry of Internal Affairs, 2012. 83 p. (In Russ.).

3 Belokurov S.V., Skryl' S.V., Joghan V.K. et al. Model ii algoritmy avtomatizirovannogo kntrolya effektivnosti system zashchity informatsii [The models and algorithms for the automated control of the effectiveness of information security systems in automated systems: monograph]. Voronezh, Voronezh Institute of the Russian Interior Ministry, 2012. 116 p. (In Russ.).