Методический подход к оценке вероятностей реализации угроз безопасности информации

Рассмотрена проблема оценки эффективности обеспечения защиты информации. Предложено описывать показатели эффективности защиты информации в IT-системах статистической мерой, для вычисления которой целесообразно использовать вероятностную модель исходов, возможных при вычислении обобщенных функций обеспечения безопасности информации.

Ключевые слова: информационная безопасность, показатели эффективности защиты информации, вероятностная модель.

Введение. Анализ современных публикаций показывает, что ряд мировых государств проводит научно-практические исследования по проблеме безопасности национального киберпространства [1-6]. Изыскания в данной области давно вышли на новый уровень и привели к формированию в некоторых странах принципиально новых подходов к строительству системы защиты киберпространства и его использованию в целях обеспечения национальной безопасности.

Сложность оценки эффективности обеспечения безопасности информации обусловлена неопределенностью режимов и характера эксплуатации объектов информационных технологий (ОИТ) и средств защиты информации (СЗИ). Это связано с отсутствием полных данных обо всех режимах их функционирования в реальной среде и неопределенностью, вызванной появлением различных видов угроз, а также развитием технических средств воздействия на информационные ресурсы потенциальным нарушителем (противником) и возможностью появления новых способов и средств нарушения информации (новых угроз).

Данные факторы носят случайный (стохастический) характер. Следовательно, показатели эффективности защиты информации в ОИТ лучше всего описывать статистической мерой, для вычисления которой целесообразно использовать вероятностную модель исходов, возможных при решении обобщенных функций обеспечения безопасности информации.

Теоретический анализ. Создание и использование информационных систем в различных областях жизнедеятельности привели к возникновению новых проблем в сфере безопасности личности, общества и государства. Внимание к этим вопросам закономерно. Если организация допускает утечку более 20 % важной внутренней информации, то она в 60 случаях из 100 банкротится [7]. Утверждают также [8], что 93 % компаний, лишившихся доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно.

Потребность в обеспечении информационной безопасности связана с тем, что существует множество субъектов и структур, весьма заинтересованных в чужой информации и готовых заплатить за это высокую цену. Так стоимость устройств подслушивания, продаваемых только в США, составляет в среднем около 900 млн долл. в год. Суммарный урон, нанесенным организациям по отношению, к которым осуществлялось

прослушивание, составляет в США около 6 млдр. долл. ежегодно. Существуют и, соответственно, приобретаются устройства для несанкционированного доступа к информации и по другим каналам: проникновение в информационные системы, перехват и дешифровка сообщений и т. д. В результате, по данным SANS Institute, в США средний размер убытков от одной атаки на корпоративную систему для банковского и ИТ-секторов экономики составляет около полумиллиона долларов [9]. Примерная структура последствий неэффективного обеспечения информационной безопасности в американских организациях такова [8]: кража конфиденциальной информации - 20-25% от общего годового ущерба; фальсификация финансовой информации - 21-25%; заражение вредоносными программами - 11-12%; нарушение доступа к web-сайтам - 1-11%; срыв работы информационной системы - 4-10%; незаконный доступ сотрудников к информации - 4-9%; другие виды ущерба - 14-33%.

В таких условиях все более широко распространяется мнение, что защита информации должна по своим характеристикам быть соразмерной масштабам угроз [10,11,12]. Отклонение от этого правила чревато дополнительным ущербом. Скажем, если уровень защищенности информационной системы превышает уровень С2 по «Оранжевой книге», то ее подсистема защиты потребляет значительную часть общих ресурсов (для систем уровня В1 эта доля составляет 20-50%, а для уровня В2 она может превышать 90%) [8]. Для каждой системы имеется оптимальный уровень защищенности, который и нужно поддерживать [2].

По статистическим данным Национального отделения ФБР по компьютерным преступлениям, от 85 до 97% нападений на корпоративные сети не только не пресекаются, но даже не обнаруживаются. Специальная группа экспертов провела анализ защищенности 8932 военных информационных систем; в 7860 (88%) случаях несанкционированное проникновение посторонних в эти системы было успешным. Администраторы только 390 из них обнаружили атаки, и всего лишь 19 сообщили о них.

Сведений об аналогичных по масштабу проверках эффективности СЗИ, проведенных в Республике Беларусь, нет, но можно предположить, что реальный уровень обеспечения информационной безопасности у нас вряд ли выше.

Нет сомнений, что защита критически важных объектов информационных систем находится на соответствующем уровне. Применяются дорогостоящие технические средства и внедряются строго регламентированные организационные мероприятия.

Однако нет ответа на самый важный вопрос - насколько предлагаемое или уже реализованное решение хорошо, какова его планируемая или реальная эффективность. Такому положению, сложившемуся сейчас в информатике, но невозможному в области обеспечения интегрированной безопасности объектов традиционной инженерии (например, таких, как авиация, транспорт или энергетика), есть ряд причин:

- игнорирование системного подхода как методологии анализа и синтеза СЗИ;

- отсутствие механизмов полного и достоверного подтверждения качества СЗИ;

- недостатки нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев.

Результаты и их обсуждение. Исходя из вышеизложенного, в качестве показателя эффективности защиты информации предлагается использовать вероятность предотвращения угрозы (вероятность обеспечения безопасности информации):

$$P = \prod_{i=1}^{l}(1 - P_i), \quad (1)$$

где P_i – вероятность реализации i-й угрозы;

l – общее число возможных угроз.

В качестве интегрального показателя эффективности защиты информации предлагается использовать степень защищенности ОИТ от комплекса угроз за заданное время t:

$$P = \prod_{i=1}^{l}(1 - K_i\ t\ P_i\ t\ ), \quad (2)$$

где $K_i(t)$ – коэффициент опасности угрозы, определяемый в виде четких или нечётких множества для каждой угрозы соответственно.

Целесообразно в качестве показателя эффективности защиты информации рассмотреть и средний риск принятия определенных состояний ОИТ при воздействии угроз:

$$R = \sum_{j=1}^{9} R_j\ x = \sum_{j=1}^{9} \prod_{i=1}^{l} C_{ji} P_{ji} P_i, \quad (3)$$

где P_i – вероятность появления угрозы i-го класса;

P_{ij} – априорная вероятность j – го состояния объекта оценка(ОО) при воздействии угрозы i-го классы;

C_{ij} – потери ОО при принятии им j-го состояния в случае воздействия угрозы i-го класса;

j – одно из состояний ОИТ, соответствующее одному из возможных событий, которые составляют полную группу несовместимых событий при воздействии угроз. Этим событиям соответствуют определённые возможные состояния ОИТ.

В случае если состояния ОО$j = k, k = 1{,}4$, при которых СЗИ устраняют воздействие угроз и обеспечивается безопасность информации, приносят нулевые потери, вероятность обеспечения безопасности информации будет определяться выражением

$$P_o = \prod_{i=k} \prod_{i=1}^{l} P_{ji} P_i. \quad (4)$$

Вероятности P_{ji} от используемого комплекса мероприятий, методов обеспечения безопасности информации и программно-аппаратных средств защиты информации, образующих СЗИ (вариант защиты z), т. е. $P_{ji} = f(z) = P_{jiz}$,так же как и вероятности $P_i = f(z) = P_{iz}$в выражениях (1) и (2).

Следовательно, справедливо равенство

$$P_{oiz} = 1 - P_{iz} = \prod_{i=k} P_{jiz} P_i, \quad (5)$$

где P_{oiz} - вероятность обеспечения безопасности информации от i-й угрозы при z-м варианте защиты информации.

Отсюда следует, что вероятность реализации i-й угрозы будет определяться выражением

$$P_{iz} = 1 - \prod_{j=k} P_{jiz} P_i. \quad (6)$$

Вероятность обеспечения безопасности информации от воздействия угроз будет определяться выражением

$$P_z = \prod_{i=1}^{l} (1 - \prod_{j=k} P_{jiz} P_i). \quad (7)$$

Тогда оптимальная стратегия принятия решения о выборе варианта защиты информации, обеспечивающего минимум вероятности реализации угроз, сводится к решению вида

$$z = \underset{z}{argmax} P_z = \underset{z}{argmax} \prod_{i=1}^{l} (1 - \prod_{j=k} P_{jiz} P_i \ . \quad (8)$$

Аналогичные результаты можно получить с использованием (2). Однако в этом случае, если состояния ОО $j \neq k, k = 5, n$, при которых СЗИ не устраняют воздействие угроз, вероятность реализации угроз (вероятность нарушения безопасности информации) будет определяться выражением

$$P_н = \prod_{i=k} \prod_{i=1}^{l} P_{ji} P_i. \quad (9)$$

Критерий (9) является оптимальным в смысле минимизации вероятности нарушения безопасности (максимизации вероятности обеспечения безопасности) информации. Отсюда следует, что возможность реализации i-й угрозы при варианте защиты z будет определяться выражением

$$P_н = \prod_{i=k} P_{jiz} P_i. \quad (10)$$

Вероятность обеспечения безопасности информации от воздействия угроз будет определяться выражением

$$P_z = \prod_{i=1}^{l} (1 - K_i(t) \prod_{j=k} P_{jiz} P_i). \quad (11)$$

Максимизация критерия (11) приводит к оптимальной стратегии принятия решения о выборе варианта защиты информации, обеспечивающего максимальную степень защищенности (минимум вероятности реализации угроз с учетом коэффициента опасности угроз), т. е. к решению вида

$$z = \underset{z}{argmax} P_z = \underset{z}{argmax} \prod_{i=1}^{l} (1 - K_i(t) \prod_{j=k} P_{jiz} P_i \ . \quad (12)$$

Заключение. На наш взгляд, перспективным направлением исследований по развитию методологии организации комплексной защиты информации являются использование аппарата статистической теории принятия решений и разработка на его базе эффективных алгоритмов количественной оценки защищенности информации на объектах информатизации, обоснования требований к средствам и системам защиты, а также выбора варианта защиты информации с учетом его стоимости, что будет освещено в последующих публикациях на страницах журнала.

Литература

1. **Шариков, П.А**. США хотят быть планетарным модератором. Американская глобальная стратегия развития киберпространства в полицентричном мире / П.А Шариков // Зарубежное военное обозрение. - 2011. - № 2. - С. 54-59.

2. **Казаковцев, А.В.** НАТО и кибербезопасность / А.В. Казаковцев // Вестник Волгоградского государственного университета - 2012. - № 2 - С. 109-114.

3. **Безкоровайный, М.М**. Кибербезопасность - подходы к определению понятия / М.М. Безкоровайный // Вопросы кибербезопасности. - 2014. - № 1. - С. 22-27.

4. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю.В. Бородакий [и др.] // Вопросы кибербезопас- “ности. - 2014. - № 1. - С. 2-8.

5. **Туляков, О.** Информационная война в планах Пентагона / О. Туляков // Зарубежное военное обозрение. - 2015. - № 11. - С. 3-14.

6. **Колосков, С.** Стратегия действий министерства обороны США в киберпространстве / С. Колосков // Зарубежное военное обозрение. - 2016. - № 10. - С. 3-7.

7. **Сабынин, В.** Специалисты, давайте говорить на одном языке и понимать друг друга / В. Сабынин // Информост - Средства связи. - № 6.

8. **Сэйер, П**. Lloyd страхует от хакеров / П. Сэйер // Computerworld Россия. - 2000. - № 30.

9. **Хмелев, Л.С.** Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем / Л.С. Хмелев // Безопасность информационных технологий: материалы науч.-технич. конф., Пенза, июнь 2001 г. - С. 55-60.

10. **Баутов, А.** Стандарты и оценка эффективности защиты информации / А. Баутов // Стандарты в проектах современных информационных систем: материалы III Всероссийской практ. конф., Москва, 23-24 апр. 2003 г.

11. **Баутов, А.** Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. - 2002. - № 2.

12. Практические рекомендации по информационной безопасности / С. Вихорев, А. Ефимов // Jet Info - 1996.-Ns 10-11.

The effectiveness of assessment of protection information support is considered. It is proposed to describe the information protection efficiency indicators of IT systems by a statistical measure, for the calculation of which it is expedient to use the probabilistic model of outcomes possible at calculation of generic functions for ensuring information security.