УДК 004.942

АНАЛИЗ УСТОЙЧИВОСТИ ДИНАМИЧЕСКОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ВЕРОЯТНОСТНО-ЭНТРОПИЙНОГО ПОДХОДА

Мирошина И.Е.[1], Чулюков В.А.[1]

[1]ФГБОУ ВПО «Воронежский Государственный педагогический университет», Воронеж, Россия (394043, Воронеж, ул. Ленина, 86), e-mail: chul_130451@mail.ru

Рассматривается анализ возможностей вероятностно-энтропийной модели системы безопасности информации в вычислительных сетях для исследования устойчивости системы к внешним воздействиям. Задача вызвана необходимостью формализации процесса динамической безопасности информации в условиях непрерывного эволюционирования динамики средств защиты и средств воздействия на них для разнородных вычислительных сетей. Показано, что распределение в вычислительных сетях средств защиты по перекрытию источников угроз безопасности информации будет определять (по У.Р. Эшби) структурное разнообразие системы при заданной политике безопасности, а значит и количественную меру неопределенности результата взаимодействия средств защиты информации и средств неправомерного доступа. Дана интерпретация закона Эшби о требуемом разнообразии для средств защиты информации и средств неправомерного доступа.

Ключевые слова: модель, безопасность информации, вычислительные сети

STABILITY ANALYSIS OF DYNAMIC SYSTEM INFORMATION SECURITY BASED ON PROBABILISTIC-ENTROPY APPROACH

Miroshina I.E.[1], Chulyukov V.A.[1]

[1]Voronezh State Pedagogical University, Voronezh, Russia (394043, Voronezh, Lenin Str., 86), e-mail: chul_130451@mail.ru

Discusses the analysis of capabilities of the probabilistic-entropy model of information security in computer networks to investigate the stability of the system to external influences. The problem is caused by need of formalization of process of dynamic safety of information in the conditions of a continuous evolution of dynamics of means of protection and means of influence on them for heterogeneous computer networks. It is shown that the distribution in computer networks remedies for overlap of the sources of threats to information security will determine (by W.R. Ashby) structural diversity of system for a given security policy and, therefore, a quantitative measure of uncertainty of the result of interaction of means of protection and the means of unauthorized access. Ashby Law of the required diversity is interpreted for the protection means of information and for the means of unauthorized access.

Keywords: model, information security, computer network

Динамическую систему безопасности информации в вычислительных сетях можно представить в виде взаимовлияющих множеств: системы средств защиты информации (ССЗИ), средств воздействия, угроз, неправомерных действий (СНД) и отношений взаимовлияния отдельных компонентов систем средств защиты информации и средств воздействия [1]. Будем считать, что воздействия СНД являются внешними по отношению к СЗИ, то есть будем учитывать влияние процессов системы угроз на процессы, происходящие как с ССЗИ в целом, так и с ее компонентами в отдельности и с самой защищаемой информацией. Кроме того, эти внешние воздействия могут быть постоянными или изменяться во времени. Устойчивость в этом случае необходимо определять как свойство системы по поддержанию отклонений выходных параметров СЗИ относительно

эталонных значений в пределах заданных малых величин при воздействии на систему средствами неправомерного доступа [2].

Цели и методы

Целью работы является анализ возможностей вероятностно-энтропийного подхода для исследования устойчивости к внешним воздействиям системы безопасности информации в вычислительных сетях.

В процессе эволюции ССЗИ уровень знаний СНД о ССЗИ в начальный период минимален, а время сбора и анализа аналитической службой системы «неправомерных действий» информации о ССЗИ (τ_{Δ}) является величиной случайной. Следовательно, защищаемая информация недоступна и ССЗИ устойчива к воздействиям СНД. Определим значения следующих временных интервалов:

- $\tau_{\triangleleft}$ - интервал, в течение которого обученность СНД по преодолению (вскрытию) СЗИ, однотипных с данной, растет; темпы преодоления ССЗИ увеличиваются; вероятность неправомерных действий по отношению к защищаемой информации через ССЗИ такой структуры увеличивается;
- $\tau_{\triangleright}$ - интервал, в течение которого ССЗИ перестает выполнять свои функции вследствие морального старения, недоступность ССЗИ падает; информация доступна СНД и ССЗИ неустойчива к его воздействиям.

Будем считать, что величины временных интервалов $\tau_{\Delta}, \tau_{\triangleleft}, \tau_{\triangleright}$ зависят от следующих свойств СЗИ и СНД:

- «разнообразие» ($d(\varepsilon)$) средств защиты информации;
- «обученность» – способность системы неправомерных действий к приобретению навыков по преодолению средств защиты ($t(\varepsilon)$).

В данном подходе свойства «разнообразие» и «обученность» (СЗИ и СНД соответственно) зависят от параметра ε, так что последний можно назвать «параметрическим разнообразием» системы <*средства защиты, средства воздействия*>.

Очевидно, что чем больше значение параметра ε ССЗИ, тем меньше вероятность несанкционированного доступа к защищаемой информации, а с ростом значения параметра ε СНД вероятность несанкционированного доступа к защищаемой информации увеличивается.

Значения параметра ε для СЗИ формируется из следующих параметров: длина ключа криптографической защиты, набор символов паролевой защиты, количество операторов программного средства защиты и количество условных и безусловных переходов в них,

структуры вычислительной сети и т.п. Значения параметра ε для СНД формируется из следующих параметров: количество лиц-участников СНД, количество средств воздействия у лиц-участников СНД, наличие дополнительных обходных путей преодоления средств защиты, наличие новых программно-технических средств формирования каналов неправомерного доступа к информации (КНД), структуры вычислительной сети и т.п.

Рассмотрим подробнее влияние структуры вычислительной сети на параметр ε. В дальнейшем будем считать, что в вычислительной сети имеется N источников угроз безопасности информации или каналов неправомерного доступа (КНД), перекрытых средствами защиты, причем общее количество средств защиты обозначим как Q_N. Распределение в вычислительных сетях средств защиты по перекрытию источников угроз безопасности информации будет определять так называемое (по терминологии У.Р. Эшби [4]) «структурное разнообразие» системы при заданной политике безопасности информации (далее системы ПБИ). То есть структурное разнообразие – это количественна мера неопределенности результата взаимовлияния СЗИ и СНД.

Переходя к соответствующей терминологии, приведенное выше, можно сформулировать следующим образом. Пусть внешнее ограничение (N каналов неправомерного доступа, перекрытых Q_N средствами защиты) задает множество из N возможных состояний системы. Внутренняя же структурная организация выступает в виде вероятностной меры, определенной на этом множестве: вероятность перекрытия i-го КНД q_i-м СЗИ равна q_i / Q_N. Тогда структурное разнообразие H можно представить в виде:

$$H = -\sum_{i=1}^{N} \frac{q_i}{Q_N} \ln \frac{q_i}{Q_N} \qquad (1)$$

Для случая, когда все средства защиты равновероятно распределены по всем существующим КНД, действия СНД по преодолению ССЗИ или ее любого элемента имеют максимальную неопределенность и непредсказуемость, структурное разнообразие максимально. Следовательно, будет предприниматься попытка нахождения элемента ССЗИ, который наиболее эффективно преодолим. Однако выбор такого элемента ССЗИ находится в зависимости от набора операций, использующихся нарушителем при внешних воздействиях на СЗИ и уровня развития свойства «обученность» самого СНД.

Для случая, когда на все средства защиты имеются специальные средства их преодоления (или полный набор операций Λ по воздействию на конкретное средство защиты) или $q_i = Q_N$, мера неопределенности поведения системы ПБИ равна нулю, энтропия и структурное разнообразие минимально. Если неопределенность поведения

системы равна нулю – она неустойчива к существующему набору операций Λ, т.е. система ПБИ не отвечает заданным требованиям. Следовательно, для увеличения уровня неопределенности должно увеличиваться число N каналов неправомерного доступа к информации, перекрытых средствами защиты Q_N пропорционально возрастанию неопределенности. Мера неопределенности достигнет максимального значения, когда число распределения средств защиты по КНД равно вероятностно.

Результаты

Итак, свойства меры неопределенности поведения системы можно рассматривать как свойства энтропии системы и поэтому при выборе множества H структур системы при заданной политике безопасности информации необходимо учитывать (1).

Выводы

Таким образом, используя вероятностно-энтропийный подход и считая, с точки зрения ПБИ, что процессы СЗИ управляют системой, можно, используя закон Эшби (закон о требуемом разнообразии) сформулировать следующее. Выбранная политика безопасности информации может быть обеспечена только в том случае, если разнообразие средств защиты информации динамически восстанавливается до состояния «по крайней мере не меньше», чем разнообразие средств неправомерного доступа к информации.

С точки зрения системы неправомерного доступа закон Эшби можно интерпретировать так: успех неправомерных действий по вскрытию каналов доступа к информации тем больше, чем быстрее разнообразие средств неправомерного доступа (и в частности их «обученность») динамически восстанавливается до состояния «по крайней мере не меньше», чем разнообразие средств защиты информации.

Обобщая, можно сказать, что при таком подходе параметрические показатели системы СЗИ будут эволюционировать, если в ответ на каждое новое конкретное средство воздействия будет разработано новое средство по перекрытию этого появившегося канала неправомерного доступа. Таким образом, система средств защиты информации будет развиваться через временную неустойчивость, переходя к устойчивому функционированию системы средств защиты на новом качественном уровне.

Список литературы

1. Мирошина И.Е., Чулюков В.А. Распределенная информация, средства защиты и средства воздействия в модели вычислительной сети // Сборник научных трудов Sworld. – Т. 5. - № 3. – С. 36-39.

2. Мирошина И.Е., Сумин В.И., Чулюков В.А. Анализ устойчивости динамической системы безопасности информации на основе теоретико-множественной модели / Фундаментальные исследования. – 2014. - № 11-6. – С. 1248-1252.
3. Мирошина И.Е. Графовая модель вычислительной сети с взаимовлияющими средствами защиты информации и средствами воздействия / Международный журнал прикладных и фундаментальных исследований. – 2014. - № 3. – Часть 1. – С. 19 -21
4. Эшби У.Р. Введение в кибернетику. – М.: Издательство иностранной литературы, 1959. – 432 с.
5. Туровец О.Г. Теория организации / Учебное пособие О.Г.Туровец, В.Н. Родионова. – М.: Инфра, 2004. – 128 с.

Рецензенты:

Сумин В.И., д.т.н., профессор, профессор кафедры управления и информационно-технического обеспечения Федерального казенного образовательного учреждения высшего профессионального образования «Воронежский институт Федеральной службы исполнения наказаний», г. Воронеж;

Астахова И.Ф., д.т.н., профессор, профессор кафедры математического обеспечения ЭВМ Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Воронежский государственный университет», г. Воронеж.