КОМПЛЕКСНАЯ ОЦЕНКА ЗАЩИЩЕННОСТИ ВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

Т.А. АНДРИЯНОВА, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 12 сентября 2017

Аннотация. В представленной статье рассматриваются методики комплексной оценки защищенности ведомственных информационных сетей (ВИС). Объекты и методики контроля ВИС определяются с учетом условий и специфики деятельности государственных органов. В данной работе предложена методика оценки информационной безопасности ВИС на основе теоретико-графовых моделей и экспертная методика оценки возможности реализации угроз.

Ключевые слова: система защиты информации, графовые модели, угроза, информационная безопасность, вероятность.

Abstract. The methods of comprehensive security estimation of departmental networks are examined. Objects and methods of monitoring of the departmental networks defined by taking into account the conditions and the specific activity of the state bodies. The method for evaluation of information security of departmental networks based on the theoretical graph models and expert security risks assessment are proposed in this article.

Keywords: information security system, graph models, threats, information security, probability.

Doklady BGUIR. 2017, Vol. 109, No. 7, pp. 40-44
Comprehensive security estimation of departmental networks
T.A. Andryianava, S.B. Salomatin

Введение

Сложность и многообразие реальных процессов в области информационной безопасности предполагают использование комплекса сетевых моделей. Информационно-технический уровень моделирования систем безопасности включает построение и оптимизацию сетей информационного обмена, разведку и защиту сетей, построение сети информирующих средств в условиях конфликта. В этих условиях особое значение имеют системы информационной безопасности (ИБ) ведомственных информационных сетей (ВИС), созданных для производственных и специальных потребностей органов государственной власти.

Объекты и методики контроля ВИС определяются с учетом условий и специфики деятельности государственных органов. В данной работе предложены методика оценки безопасности ИБ ВИС на основе графовых моделей и экспертная методика оценки возможности реализации угроз.

Модели комплексной оценки защищенности сетей

Сеть представляется трехдольным графом $G(P, O, Z, E, H)$ (рис. 1), включающим [1–3]:
– множество угроз P ($p_1, p_2, \ldots, p_N$)
– множество объектов защиты O ($o_1, o_2, \ldots, o_L$);
– множество воздействий угроз на объекты E ($e_1, e_2, \ldots, e_K$);
– множество средств и механизмов защиты Z ($z_1, z_2, \ldots, z_M$);
– множество воздействий системы защиты информации на угрозы H ($h_1, h_2, \ldots, z_j$).

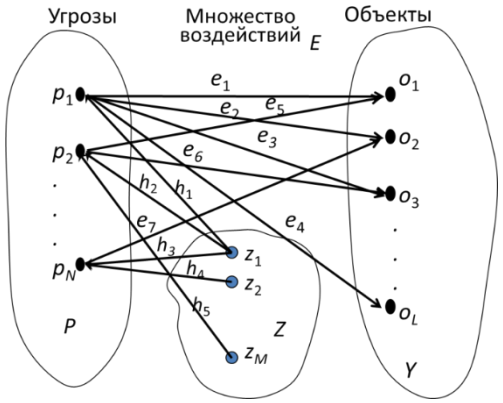

Рис. 1. Модель системы с полным перекрытием – на каждую угрозу есть нейтрализующее средство защиты информации

Каждое ребро графа G (P, O, Z, E, H) специфицирует воздействие конкретной угрозы на конкретный объект. От каждой угрозы может быть несколько воздействий на различные объекты, и каждый объект может быть подвергнут нескольким угрозам.

Граф G (P, O, Z, E, H) относится к классу взвешенных графов. Веса вершин и ребер позволяют учитывать величину ущерба от реализации угроз и вероятность осуществления угроз. Выбор защитных механизмов осуществляется так, чтобы, редуцируя граф, устранить наиболее опасные угрозы или изменить веса e_i с тем, чтобы минимизировать поток угроз на основе тех или иных критериев.

Представим взвешенный граф G (P, O, Z, E, H) следующей совокупностью векторов и матриц:

– вектор P (p_1, p_2,…, p_N) где p_i – вероятность осуществления соответствующей угрозы;

– вектор O (o_1, o_2, … , o_L) где o_i – стоимость соответствующего объекта защиты;

– $N \times L$ матрица $E\{e_{i,j}\}$, где элемент $e_{i,j} = 1$ при воздействии i-й угрозы на j-й объект и равен 0 в противном случае;

– вектор Z (z_1, z_2, … , z_M), где z_i – стоимость соответствующего способа или средства защиты;

– $N \times M$ матрица $H\{h_{i,j}\}$, где $h_{i,j}$ – вероятность устранения (или степень снижения ущерба) i-й угрозы от применения j-го средства защиты.

Ущерб безопасности без использования системы защиты информации можно оценить из выражения [3]:

$$U = \sum_{i=1}^{L} o_i (1 = \prod_{j=1}^{N} e_{i,j} (1 - p_j)). \quad (1)$$

Ущерб безопасности при использовании системы защиты информации в условиях независимых воздействий определяется согласно выражению

$$U_{\text{ÑÇÈ}} = \sum_{i=1}^{L} o_i (1 = \prod_{j=1}^{N} e_{i,j} (1 - p_j (1 - \prod_{k=1}^{M} (1 - h_{j,k})))). \quad (2)$$

Выигрыш от применения системы защиты информации равен

$$\acute{Y} = (U - U_{\text{ÑÇÈ}}) / (\sum_{i=1}^{L} o_i - \sum_{k=1}^{M} z_k). \quad (3)$$

Вероятность реализации независимых угроз без использования системы защиты информации оценивается как

$$Pr_{\text{óãð}} = 1 - \prod_{i=1}^{N} (1 - p_i), \quad (4)$$

при этом вероятность преодоления системы защиты равна

$$P_{\text{ï ð}} = 1 - \prod_{i=1}^{N} (1 - p_i (1 - \prod_{k=1}^{M} (1 - h_{i,k}))). \quad (5)$$

Модель системы защиты, которая учитывает возможные недостатки в системе безопасности, приведена на рис. 2 [2].

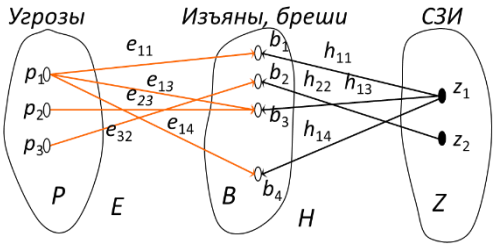

Рис. 2. Модель комплексной оценки защищенности сети с учетом изъянов в системе безопасности

Модель системы безопасности представляет собой взвешенный трехдольный граф G (P, B, Z, E, H), где E– матрица вероятностей осуществления угроз по брешам в системе безопасности; H – матрица вероятностей нейтрализации (степени устранения) с помощью системы безопасности.

Комплексная оценка защищенности предполагает прохождение следующих этапов:

1) идентификация и определение ценности объектов защиты;

2) формирование перечня угроз и оценка их опасностей (вероятностей) на основе видового дерева;

3) формирование «Перечня системы защиты» – базового уровня защиты с учетом нормативных требований на основе видового дерева (рис. 3);

4) вычисление ущерба с учетом применения системы защиты и оценка остаточного риска, как правило, в ранговой шкале на основе экспертной методики оценки возможности реализации угрозы;

5) формирование дополнительных мер защиты и системы защиты информации (СЗИ) для достижения приемлемого риска.

Определение ценности объектов защиты осуществляется в большинстве методик на основе материальной стоимости и ущерба от их разрушения, несанкционированного доступа [4–7].

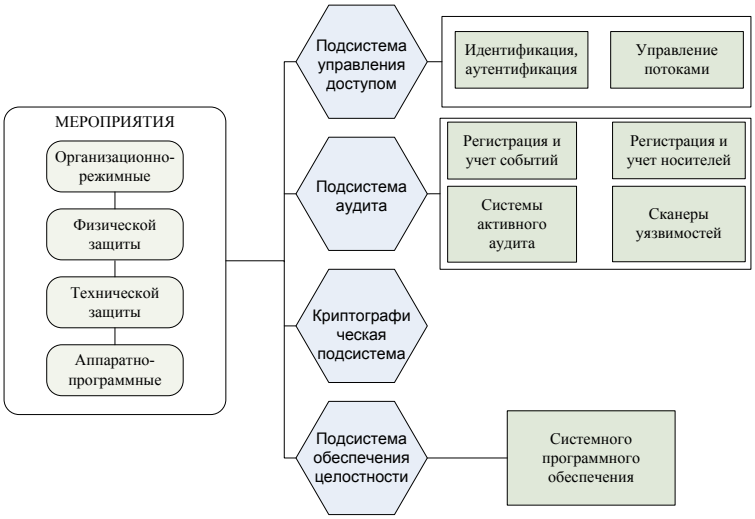

Рис. 3. Схема формирования «Перечня системы защиты»

Определение опасности или вероятностей угроз в большинстве методик проводится на основе экспертных оценок и анализа имеющейся статистики.

Экспертная методика оценки возможности реализации угрозы

В основе методики лежит понятие угрозы информационной безопасности, которое характеризуется объектом, субъектом, источником и проявлением, поэтому оценку возможности ее реализации на элементе ВИС предлагается осуществлять с помощью следующих показателей [4–7]:

1) $\delta_{\text{äîñò}}(t)$ – дельта-функция доступности ВИС для нарушителя, принимающая значение 1, если площадь зоны покрытия сети превышает площадь контролируемой зоны, и 0 в противном случае;

2) $K_{\text{íí}}(t)$ – коэффициент опасности нарушителя;

3) $P_{OS_{\text{î ñÇ}}}(1/\delta)$ – возможность преодоления системы защиты;

4) $P_{OS_{\text{àî}}}(t/y)$ – возможность реализации атаки на объект без системы защиты.

Возможность реализации $P_{OS_{\text{ðó}}}(t/y)$ угрозы информационной безопасности ВИС, наносящей ущерб определенной величины за определенный интервал времени *t*, может быть вычислена по следующей формуле:

$$P_{OS_{\text{ðó}}}(t) = \delta_{\text{äîñò}}(t) K_{\text{î í}}(t) P_{OS_{\text{î ñÇ}}}(1/\delta) P_{OS\text{àî}}(t/y). \quad (6)$$

Коэффициент опасности нарушителя $K_{\text{î í}}(t)$ принимает значения на интервале [0, 1], причем для нарушителей, представляющих наименьшую опасность, этот показатель стремится к нулю. Коэффициент $K_{\text{î í}}(t)$ характеризует нарушителя как субъекта угрозы, сопоставленной с его потенциалом:

$$K_{\text{î í}}(t) = P_{OS_{\text{í í}}}(t)\Pi, \quad (7)$$

где $P_{OS_{\text{í í}}}(t)$ – возможность наличия злоумышленника; П – потенциал злоумышленника.

Под $P_{OS_{\text{í í}}}(t)$ понимается вероятность, отражающая мнение эксперта о существовании нарушителя определенного класса для конкретной ВИС за определенный интервал времени.

Потенциал злоумышленника также принимает значения на интервале [0, 1] и характеризует опасность нарушителя с точки зрения его квалификации, технической оснащенности и осведомленности о структуре ВИС.

Возможность преодоления системы защиты $P_{OS_{\text{î ñÇ}}}(1/\delta)$ связывают с многоэтапной структурой проводимых атак. Нарушитель может реализовать некоторую угрозу безопасности только после успешного завершения попытки преодолеть применяемые в сети средства защиты. Атаки совершаются непосредственно на ядро сети и циркулирующую в ней информацию. Поэтому для определения $P_{OS_{\text{î ñÇ}}}(1/\delta)$ необходимо предварительно оценить возможность реализации атак на применяемую в сети систему защиты при условии доступности сети.

Возможность реализации атаки на объект $P_{OS_{\text{î ñÇ}}}(t/y)$ характерна для второго этапа атак на ВИС (при условии успешного преодоления средств защиты), и ее надо рассматривать как проявление угроз информационной безопасности с точки зрения вероятности выполнения деструктивного действия при реализации каждой угрозы.

В результате применения предложенной методики могут быть получены оценки возможности реализации каждой из выявленных угроз информационной безопасности ВИС, следствием которых является нанесение ущерба определенной величины.

Заключение

Рассмотрены методики комплексной оценки защищенности ведомственных информационных сетей на основе теоретико-графовой сетевой модели и экспертной оценки знаний. Применение методик позволит проводить оценку степени реализации функциональных требований (сертификация по требованиям безопасности), в том числе возможных уязвимостей, брешей безопасности.

Результаты оценки могут стать основой для проведения аналитической работы и подготовки предложений, направленных на выработку конкретных мероприятий по совершенствованию системы защиты информации.

Список литературы

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000. 452 с.
2. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Екатеринбург, ИОНЦ «Информационная безопасность», 2008. 212 с.
3. Корт С.С. Теоретические основы защиты информации. М.: Гелиос АРВ, 2004. 240 с.
4. Девянин П.Н. Модели безопасности компьютерных систем. М.: Изд. центр «Академия», 2005. 144 с.
5. Новоселов А.А. Математическое моделирование финансовых рисков. Теория измерения. Новосибирск:

Наука, 2001. 102 с.
6. Батаронов И.Л., Паринов А.В., Симонов К.В. Оценка и регулирование рисков, обнаружение и предупреждение компьютерных атак на инновационные проекты // Информация и безопасность. 2013. Т. 16, вып. 2. С. 243–246.
7. Бутузов В.В., Заряев А.В. К вопросу обоснования функции ущерба атакуемых систем // Информация и безопасность. 2013. Т. 16, вып. 1. С. 47–54.

References

1. Zegzhda D.P., Ivashko A.M. Osnovy bezopasnosti informacionnyh sistem. M.: Gorjachaja linija – Telekom, 2000. 452 s. (in Russ.)
2. Gajdamakin N.A. Teoreticheskie osnovy komp'juternoj bezopasnosti. Ekaterinburg, IONC «Informacionnaja bezopasnost'», 2008. 212 s. (in Russ.)
3. Kort S.S. Teoreticheskie osnovy zashhity informacii. M.: Gelios ARV, 2004. 240 s. (in Russ.)
4. Devjanin P.N. Modeli bezopasnosti komp'juternyh sistem. M.: Izd. centr «Akademija», 2005. 144 s. (in Russ.)
5. Novoselov A.A. Matematicheskoe modelirovanie finansovyh riskov. Teorija izmerenija. Novosibirsk: Nauka, 2001. 102 s. (in Russ.)
6. Bataronov I.L., Parinov A.V., Simonov K.V. Ocenka i regulirovanie riskov, obnaruzhenie i preduprezhdenie komp'juternyh atak na innovacionnye proekty // Informacija i bezopasnost'. 2013. T. 16, vyp. 2. S. 243–246. (in Russ.)
7. Butuzov V.V., Zarjaev A.V. K voprosu obosnovanija funkcii ushherba atakuemyh sistem // Informacija i bezopasnost'. 2013. T. 16, vyp. 1. S. 47–54. (in Russ.)

Сведения об авторах

Андриянова Т.А., аспирант кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Саломатин С.Б., к.т.н., доцент кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, д. 6,
Белорусский государственный университет
информатики и радиоэлектроники
тел. +375-17-293-88-33;
e-mail: kafsiut@bsuir.by
Саломатин Сергей Борисович

Information about the authors

Andryianava T.A., PG student of the department of infocommunication technologies of Belarusian state university of informatics and radioelectronics.

Salomatin S.B., PhD, associate professor of the department of infocommunication technologies of Belarusian state university of informatics and radioelectronics.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university of
informatics and radioelectronics
tel. +375-17-293-88-33;
e-mail: kafsiut@bsuir.by
Salomatin Sergey Borisovich