УДК 004.942, 51-74, 519.857.3

И.В. Бордак, А.П. Росенко

Разработка метода количественной оценки и прогнозирования безопасности информации ограниченного доступа на основе Марковских случайных процессов

Разработаны метод и программная реализация для определения вероятностей последствий от реализации злоумышленником угроз безопасности информации ограниченного доступа (ИОД) на основе Марковских случайных процессов (МСП) при воздействии на автоматизированную информационную систему (АИС) зависимых угроз. Предложенный метод и программное обеспечение на основе МСП показали возможность реализовать количественную оценку безопасности ИОД, что позволит, используя полученные данные, разрабатывать научно обоснованные организационно-профилактические мероприятия по повышению уровня защищенности ИОД. Разработанные и обоснованные практические рекомендации при реализации собственниками ИОД обеспечат повышение защищенности информации, минимизацию материального ущерба за счет выбора оптимальных стратегий, применяемых методов и средств защиты ИОД.

Ключевые слова: безопасность информации, угрозы, математическая модель, математическое моделирование, Марковские случайные процессы.
doi: 10.21293/1818-0442-2017-20-4-67-70

Обеспечение безопасности ИОД всегда было и остается одной из важнейших проблем защиты информации (ЗИ). В результате утечки ИОД наносится значительный материальный и моральный ущерб не только собственнику такой информации, но и государству в целом [1]. Сложность проблемы обеспечения безопасности ИОД состоит в том, что ее решение зависит от многочисленных факторов, реализуемых на всех стадиях проектирования, создания и эксплуатации (АИС). В настоящее время вследствие ряда объективных причин, в первую очередь экономических, сложилась ситуация, когда теоретические разработки и применяемые методы и средства ЗИ ориентированы в основном на получение качественных характеристик. Проблема усугубляется априорной недостаточностью исходной информации, что сдерживает применение количественных методов оценки безопасности ИОД. А это, в свою очередь, порождает отставание теории безопасности ИОД от уровня развития теории ЗИ.

Большой вклад в формирование новых взглядов на актуальность проблемы, необходимость разработки и внедрения современных научно обоснованных средств, методов и технологий ЗИ внесли отечественные [1, 2] и зарубежные авторы [3, 4].

Однако, как показывает анализ, это в большей мере относится к исследованиям воздействия на АИС компьютерных вирусов, ограничению и разграничению доступа к компьютерной информации и т.п. В то же время отсутствие методов математического и компьютерного моделирования процессов и явлений, протекающих в АИС, существенно усложняет процедуру установления причинно-следственных связей при воздействии на нее дестабилизирующих факторов различной природы. Это, в свою очередь, порождает непонимание существующей проблемы как со стороны исследователей, так и собственников ИОД.

В данной работе показано, что АИС относится к сложным стохастическим человеко-машинным системам, в которой количественную оценку безопасности ИОД возможно осуществлять на основе применения к АИС Марковских случайных процессов.

Разработка метода количественной оценки и прогнозирования безопасности информации ограниченного доступа для зависимых потоков угроз

Воздействующие на АИС угрозы безопасности ИОД могут взаимно порождаться с некоторыми вероятностями r_{1i}, …, r_{in}. Поэтому предлагается принять базовую модель Марковского случайного процесса с дискретным параметром для оценки безопасности ИОД, с учетом воздействия на АИС зависимых потоков угроз. Граф состояний для модели такого типа изображен на рис. 1 [5]:

В соответствии с рис. 1 приняты следующие обозначения: q_{01}, …, q_{0i}, …, q_{0n} − вероятности возникновения i-й угрозы, характеризуют возможности злоумышленника по несанкционированному доступу к ИОД; R_{10}, …, R_{i0}, …, R_{n0} − вероятности парирования возникшей i-й угрозы, характеризующие возможности собственника ИОД по её защите; $\overline{R}_{1,n+1}$, …, $\overline{R}_{i,n+1}$, …, $\overline{R}_{n,n+1}$ − вероятности непарирования возникшей i-й угрозы силами и средствами, предпринимаемыми собственником ИОД, соответствуют поглощающему состоянию, характеризуют реализацию злоумышленником угрозы безопасности ИОД. 0, 1, ..., i, ..., n, n+1 − состояния, в которых может оказаться рассматриваемая система в результате воздействия n зависимых угроз [6].

В соответствии с рис. 1 матрица вероятностей переходов системы в различные состояния примет вид

$$\left\|\mathbf{P}_{ij}\right\| = \begin{vmatrix} 1-q_{\sum} & q_{01}\ldots & q_{0i}\ldots & q_{0n} & 0 \\ R_{10} & 0\ \ldots & r_{1i}\ \ldots & r_{1,n} & \overline{R}_{1,n+1} \\ \ldots & & & & \\ R_{i0} & r_{i1}\ldots & 0 & r_{in} & \overline{R}_{i,n+1} \\ \ldots & & & & \\ R_{n0} & r_{n1}\ldots & r_{ni}\ \ldots & 0 & \overline{R}_{n,n+1} \\ 0 & 0\ \ldots\ 0 & \ldots & 0 & 1 \end{vmatrix}. \quad (1)$$

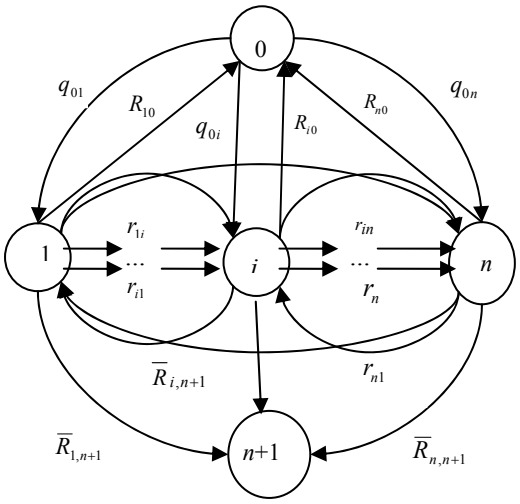

Рис. 1. Граф состояний при воздействии на АИС n зависимых потоков угроз

Матрица (1) позволяет определить вероятности переходов АИС в различные состояния.

После первого шага вероятности состояний будут равны

$$P_0(1)=1-\sum q;\quad P_1(1)=q_{01};\ \ldots;\ P_i(1)=q_{0i};\quad \ldots;\ P_n(1)=q_{0n};\quad P_{n+1}(1)=0. \quad (2)$$

После k-го шага вероятности состояний примут следующий вид:

$$P_0(k)=\sum_{j=0}^{n+1}P_j(k-1)P_{j0}=P_0(k-1)P_{00}+P_1(k-1)P_{10}+\ldots+P_j(k-1)P_{j0}+P_n(k-1)P_{n0}+P_{n+1}(k-1)P_{n+1,0};$$

$$P_1(k)=\sum_{j=0}^{n+1}P_j(k-1)P_{j1}=P_0(k-1)P_{01}+P_1(k-1)P_{11}+\ldots+P_j(k-1)P_{j1}+P_n(k-1)P_{n1}+P_{n+1}(k-1)P_{n+1,1};$$

$$\ldots\ \ldots\ \ldots\ldots\ \ldots;$$

$$P_i(k)=\sum_{j=0}^{n+1}P_j(k-1)P_{ji}=P_0(k-1)P_{0i}+P_1(k-1)P_{1i}+\ldots+P_j(k-1)P_{ji}+P_n(k-1)P_{ni}+P_{n+1}(k-1)P_{n+1,i};$$

$$\ldots\ \ldots\ \ldots\ldots\ \ldots; \quad (3)$$

$$P_n(k)=\sum_{j=0}^{n+1}P_j(k-1)P_{jn}=P_0(k-1)P_{0n}+P_1(k-1)P_{1n}+\ldots+P_j(k-1)P_{jn}+P_n(k-1)P_{nn}+P_{n+1}(k-1)P_{n+1,n};$$

$$P_{n+1}(k)=\sum_{j=0}^{n+1}P_j(k-1)P_{j,n+1}=P_0(k-1)P_{0,n+1}+P_1(k-1)P_{1n}+\ldots+P_j(k-1)P_{j,n+1}+P_n(k-1)P_{n,n+1}+P_{n+1}(k-1)P_{n+1,n+1}.$$

Тогда после k-го шага вероятность благополучного исхода от воздействия на АИС зависимых потоков угроз определится следующим образом:

$$P_{\text{БИ}}(k)=P_0(k)+P_1(k)+\ldots+P_i(k)+P_n(k). \quad (4)$$

Вероятность неблагоприятного исхода как противоположного события будет равна

$$Q_{\text{БИ}}(k)=P_{n+1}(k). \quad (5)$$

Так как $P_{\text{БИ}}(k)$ и $Q_{\text{БИ}}(k)$ составляют полную группу событий, тогда

$$P_{\text{БИ}}(k)+Q_{\text{БИ}}(k)=1. \quad (6)$$

Выражение (6) используется как проверочное условие.

Разработка программного обеспечения

В соответствии с представленной моделью количественной оценки безопасности ИОД для зависимых потоков угроз разработаны алгоритм и программное обеспечение [5, 8]. Для реализации алгоритма выбрана система программирования Delphi, так как предоставляет наиболее широкие возможности для программирования приложений ОС Windows.

При разработке программного обеспечения в качестве входных параметров использовались:

– количество рассматриваемых угроз (N), характеризующее угрозы в актуальном на данный момент списке угроз;

– количество шагов алгоритма (K). Так как выбранный метод количественной оценки безопасности ИОД дискретен, то и сам алгоритм рассматривается по шагам (1, 2, … K);

– матрица переходных вероятностей (1), характеризующая исходный граф состояний АИС, а именно: $q_{01},\ldots,q_{0i},\ldots,q_{0n}$ – вероятность возникновения i-й угрозы; $R_{10},\ldots,R_{i0},\ldots,R_{n0}$ – вероятность парирования возникшей i-й угрозы; $\overline{R}_{1,n+1}$, ..., $\overline{R}_{i,n+1}$, ..., $\overline{R}_{n,n+1}$ – вероятность непарирования возникшей i-й угрозы; r_{ij} – вероятность того, что при реализации i-й угрозы порождается j-я угроза безопасности ИОД.

Выходные параметры программы количественной оценки безопасности ИОД следующие:

– матрица, вероятности которой характеризуют возможность системы находиться в любом из 0, 1, ..., i, ..., n, n+1 состояний на каждом из K шагов алгоритма;

– вероятности благополучного ($P_{\text{БИ}_i}$) и неблагополучного ($Q_{\text{БИ}i}$) исходов от реализации угроз, рассчитанные для каждого из K шагов алгоритма;

– графическое представление зависимости $P_{\text{БИ}_i}$ от реализованных злоумышленником угроз

безопасности ИОД и K – количества шагов алгоритма.

Исследование влияния зависимых угроз на вероятность благополучного исхода

При моделировании процесса количественной оценки безопасности ИОД для исследования влияния параметров, определяющих возможности злоумышленника по несанкционированному доступу к защищаемой информации и возможности собственника по защите ИОД на величину вероятности благополучного исхода, были рассмотрены входные параметры с разными показателями вероятностей возникновения угроз и вероятностей парирования угроз [7].

Исходные данные для моделирования представлены для четырех режимов моделирования:

– первый режим соответствует следующим исходным данным:

$$q_{01}=0{,}05,\quad q_{02}=0{,}1,\quad q_{03}=0{,}15,$$

$$R_{10}=0{,}75,\ R_{20}=0{,}8,\ R_{30}=0{,}85,$$

которые характеризуют то, что защитные возможности собственника ИОД значительно эффективнее, чем возможности злоумышленника по несанкционированному доступу к защищаемой информации;

– второй режим моделирования осуществлялся при следующих исходных данных:

$$q_{01}=0{,}2,\ q_{02}=0{,}25,\ q_{03}=0{,}3,$$
$$R_{10}=0{,}75,\quad R_{20}=0{,}8,\quad R_{30}=0{,}85,$$

которые свидетельствуют о том, что злоумышленник увеличил свои возможности по несанкционированному доступу к защищаемой информации при неизменных исходных данных, которые реализует собственник по защите ИОД;

– третий режим моделирования осуществлялся с учетом следующих исходных данных:

$$q_{01}=0{,}35,\ q_{02}=0{,}2,\ q_{03}=0{,}45,$$

$$R_{10}=0{,}5,\ R_{20}=0{,}6,\ R_{30}=0{,}7,$$

характеризующих то, что повышаются как защитные механизмы собственника ИОД, так и возможности злоумышленника по несанкционированному доступу к защищаемой информации;

– четвертый режим моделирования осуществлялся при следующих исходных данных:

$$q_{01}=0{,}25,\ q_{02}=0{,}25,\ q_{03}=0{,}25,$$

$$R_{10}=0{,}75,\ R_{20}=0{,}75,\ R_{30}=0{,}75,$$

свидетельствующих о том, что защитные возможности собственника ИОД и возможности злоумышленника по несанкционированному доступу к защищаемой информации не изменяются.

Результаты математического моделирования представлены на рис. 2.

Наиболее благоприятные исходы для собственника ИОД соответствуют первому режиму моделирования (рис. 2, испытание 1), когда у собственника информации имеются существенные преимущества по защите своих информационных ресурсов по сравнению со злоумышленником.

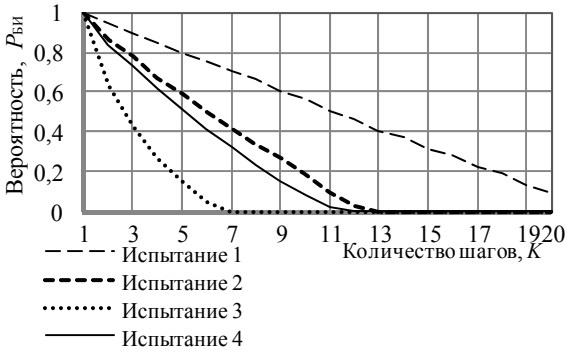

Рис. 2. Зависимость вероятности благополучного исхода от возможностей злоумышленника по несанкционированному доступу к защищаемой информации (q_{0i}), возможностей собственника по защите ИОД (R_{i0}) и K

В то же время видно (рис. 2, испытание 2), что даже незначительное увеличение возможностей злоумышленника по сравнению с испытанием 1, при неизменных защитных свойствах собственника ИОД, приводит к значительному уменьшению вероятности $P_{БИ}$. Так, в соответствии с рис. 2 уже на пятом шагу моделирования вероятность $P_{БИ}$ снижается с вероятности 0,8 до 0,59, а на девятом шагу вероятность $P_{БИ}$ снижается с 0,6 (испытание 1) до 0,28 (испытание 2).

Ещё более существенно наблюдается снижение вероятности $P_{БИ}$ для третьего режима испытания, когда защитные механизмы собственника ИОД уменьшаются. По сравнению с первым испытанием уже на пятом шагу моделирования указанная вероятность снижается с 0,8 (испытание 1) до 0,17 (испытание 3), а на девятом шагу указанная вероятность снижается с 0,6 до нуля.

Также в третьем испытании наблюдается еще более быстрое уменьшение вероятности благополучного исхода по сравнению с первыми двумя испытаниями.

Результаты четвертого режима моделирования (рис. 2, испытание 4) свидетельствуют о том, что когда защитные возможности собственника ИОД и возможности злоумышленника по несанкционированному доступу к защищаемой информации не изменяются, то вероятность $P_{БИ}$ в большей степени определяется возможностями злоумышленника по несанкционированному доступу к защищаемой информации.

Таким образом, в результате анализа проведенных исследований, изображенных на рис. 2, можно сделать следующие выводы:

– вероятность $P_{БИ}$ благополучного исхода при воздействии на АИС различных угроз безопасности ИОД от воздействия на нее угроз ИОД в значительной степени зависит как от возможностей злоумышленника по несанкционированному доступу к защищаемой информации, так и от возможностей собственника ИОД по защите своих информационных ресурсов;

– скорость снижения или роста вероятности $P_{БИ}$, как показывают результаты исследования, в большей степени определяется возможностями злоумышленника. Это обстоятельство накладывает на собственника ИОД высокую степень информированности о знаний методов и средств, применяемых злоумышленником с целью выбора и применения таких защитных механизмов, которые обеспечивают гарантированную защиту информации.

Выводы

Разработан метод количественной оценки безопасности ИОД на основе Марковских случайных процессов для зависимых угроз.

Разработано программное обеспечение для исследования количественной оценки безопасности информации ограниченного доступа на основе Марковских случайных процессов.

Проведено исследование влияния вероятности благополучного исхода с учетом воздействия на АИС зависимых угроз безопасности ИОД и возможностей по их парированию.

Учет полученных результатов моделирования позволит собственнику ИОД разрабатывать эффективные мероприятия по предупреждению неоправданного ущерба при обращении с информацией, ограниченной в распространении.

Литература

1. Введение в информационную безопасность: учеб. пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др. – М.: Горячая линия – Телеком, 2014. – 288 с.

2. Моделирование сложных атак на комплексные сети / Ф. Галиндо, Н.В. Дмитриенко, А. Карузо и др. // Безопасность информационных технологий. – 2010. – № 3. – С. 115–121.

3. Network Society: Aggregate Topological Models / A. Tikhomirov, A. Afanasyev, N. Kinash et al. // Umerov Communications in Computer and Information Science. – 2014. – Vol. 487. – P. 415–421.

4. A proposal framework for information security establishment focusing on risk evaluation and its optimum reduction based on standard. / E.A. M. Malayeri, N. Modiri, S. Jabbehdari, T. Behbahani // Advances in Information Sciences and Service Sciences. – 2012. – № 4 (7). – P. 1–11.

5. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации: методология и теоретическое исследование. – М.: КРАСАНД, 2010. – 160 с.

6. Росенко А.П. Метод определения вероятности несанкционированного доступа злоумышленника к конфиденциальной информации // Доклады ТУСУРа. – 2012. – № 1(25), ч. 2. – С. 25–28.

7. Росенко А.П. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения / А.П. Росенко, И.В. Бордак // Изв. ЮФУ. – 2015. – №7(168). – С. 7–19.

8. Свидетельство о государственной регистрации программы для ЭВМ № 2016619790 / А.П. Росенко, И.В. Бордак, Н.С. Окулов – Заявка №201661601. Дата поступления 13 июля 2016 г. Зарегистрировано в Реестре программ для ЭВМ 30 августа 2016 г.

Бордак Ирина Владимировна
Аспирант каф. прикладной математики и компьютерной безопасности (КПМКБ) института информационных технологий и телекоммуникаций
Северо-Кавказкого федерального университета
Тел.: +7-918-877-74-04
Эл. почта: irinabordak@mail.ru

Росенко Александр Петрович
Канд. техн. наук, доцент каф. КПМКБ
Тел.: +7-919-750-65-56
Эл. почта: rap.44@mail.ru

Bordak I.V., Rosenko A.P.

Development of a method for quantitative evaluation and prediction of information security with restricted access on the basis of Markov random processes

In this paper a method and software implementation are developed to determine the probabilities of the effects of the implementation of the attacker threats for the security of restricted information on the basis of Markov random processes when subjected to an automated information system of dependent threats. The proposed method and software-based Markov random processes showed the possibility to realize a quantitative evaluation of the safety the security of restricted information, which will allow using the obtained data to develop evidence-based organizational and preventive measures to improve protection of the security restricted information.
Developed and justified practical recommendations, minimize material damage due to the choice of optimal strategies, the methods and remedies the security of restricted information.
Keywords: information security, threats, mathematical model, mathematical modeling, Markov random processes.