Вычислительная техника и информационные технологии

УДК 347.775
DOI: 10.12737/23236

М.Ю. Рытов, А.П. Горлов, Д.А. Лысов

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ ЭФФЕКТИВНОСТИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ ПРИ ОДНОВРЕМЕННОЙ РЕАЛИЗАЦИИ УГРОЗ

Рассмотрена автоматизация процесса оценки эффективности комплексных систем защиты информации путем создания автоматизированной системы,основными функциями которой являются: проведение аудита информационной безопасности (ИБ), формирование модели угроз ИБ, рекомендаций по созданию системы защиты информации, комплекта организационно-распорядительной документации.

Ключевые слова: информационная безопасность, оценка эффективности, аудит ИБ, модель угроз, автоматизированная система, объект информюатизации, защищенность, аппарат сетей Петри.

M.Y. Rutov, A.P. Gorlov, D.A. Lysov

AUTOMATION OF PROCESS AN ASSESSMENT EFFICIENCY OF COMPLEX SYSTEMS OF INFORMATION SECURITY OF THE INDUSTRIAL ENTERPRISES IN CASE WITH SIMULTANEOUS IMPLEMENTATION OF THREATS

This paper reports the automation of an efficiency assessment process for complex systems of information security by means of an automated system formation the basic functions of which are: carrying out of information security (IS) audit, model formation of IS threats, recommendations for the formation of information security systems, a set of organization-regulatory documentation. For the solution of a problem in the efficiency assessment of confidential information protection there is developed a simulator and a universal criterion taking into account a probability of the realization and combating threats and allowing the estimation of the complex system efficiency for information protection in dynamics of processes occurred. The approach offered to the assessment of an information security level of an information object allows reducing considerably material and time costs for carrying out information security audit and also increasing the design solutions quality at the creation and introduction of complex system of information protection.

Key words: information security, assessment, IS audit, threats model, automated system, informatization object, security, device of Petri Nets.

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от искажения, уничтожения, хищения, разглашения конфиденциальной информации превышает миллионы рублей [1].

Согласно статистике, за 2015 год на территории РФ зафиксировано около 120 тысяч преступлений в сфере информационной безопасности. К этим преступлениям относятся неправомерный доступ к конфиденциальной информации, разглашение сведений, составляющих коммерческую тайну, создание, использование или распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

Промышленное предприятие – имущественный комплекс, используемый для осуществления предпринимательской деятельности. В состав промышленного предприятия входят все виды имущества, предназначенного для его деятельности.

Промышленные предприятия как объекты информатизации (ОИ) являются совокупностью информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений и объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [2;3].

Комплексная система защиты информации (КСЗИ) - это система, в которой действуют в единой совокупности правовые, организационные, технические, про-

граммно-аппаратные и другие подсистемы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки. Составными элементами КСЗИ являются правовая, организационная, инженерно-техническая, программно-аппаратная и криптографическая защита информации. Элементы КСЗИ, в свою очередь, в общем виде состоят из средств, устройств и способов защиты информации, а также методов их использования.

Практический опыт создания комплексных систем защиты информации на объектах свидетельствует, что чаще всего специалистам приходится дорабатывать и систематизировать уже внедренные на объекте средства и методы защиты информации. Также для поддержания высокого уровня защищенности информации необходимо периодически проводить аудит информационной безопасности и оценивать эффективность функционирования КСЗИ.

При решении рассматриваемой проблемы одной из важнейших задач является разработка математических моделей, информационного обеспечения и программного комплекса автоматизации оценки уровня защищенности и эффективности комплексных систем защиты информации[3; 5].

В основу предлагаемой методики положена оценка защищенности объекта информатизации согласно положениям законодательной базы РФ, требованиям государственных стандартов, а также проверка наличия организационно-распорядительной документации, регламентирующей защищенную обработку конфиденциальной информации.

Основной задачей разрабатываемой АС является выявление уязвимостей существующих систем обработки и защиты информации. В качестве входных данных используются данные об объекте информатизации, которые вводятся на основе специально разработанных опросных анкет.

Алгоритм работы АС (рис. 1):

- ввод исходных данных;
- формирование информационной модели объекта информатизации;
- оценка состояния защищенности ОИ;
- математическое моделирование угроз ИБ;
- формирование модели угроз ИБ;
- формирование рекомендаций по совершенствованию системы защиты информации;
- формирование организационно-распорядительной документации.

Рис. 1. Механизм работы автоматизированной системы оценки эффективности КСЗИ

Преимуществом данной методики является возможность снизить трудоемкость работ, сократить временные и материальные затраты на проведение оценки уровня информационной безопасности, повысить качество проектных решений.

Наиболее распространена практика создания единой системы защиты из разрозненных элементов, когда к уже существующей информационной среде добавляются средства защиты информации. Современные условия диктуют другой подход, который заключается в том, что информационная среда изначально проектируется с точки зрения защиты всех ее компонентов. Это предполагает возможность оценить еще на этапе проектирования целесообразность использования той или иной СЗИ, а также моделировать взаимодействие СЗИ в едином информационном пространстве [4].

Состав и функциональность проектируемой СЗИ должны соответствовать актуальным для рассматриваемой информационной системы угрозам. Для удовлетворения этого требования необходимо на этапе проектирования выявить существующие уязвимости и угрозы информационной безопасности, определить степень актуальности этих угроз и вероятность их реализации, а также возможный ущерб от их реализации. Этот этап проектирования СЗИ является одним из наиболее важных и трудоемких, так как от результата выявления угроз информационной безопасности зависит то, какими средствами будет обеспечиваться защита конфиденциальной информации.

Для автоматизации данного процесса необходимо разработать математическую модель выявления уязвимостей системы защиты информации.

Ввод исходных данных представляет собой заполнение опросных анкет, позволяющих выявить вид обрабатываемой информации, существующие средства защиты информации, угрозы ИБ, уязвимости системы защиты информации, а также прочие данные, необходимые для составления информационной модели объекта информатизации.

Следующим этапом является оценка состояния защищенности ОИ. Выделяются 3 основных направления оценки защищенности:

- оценка на соответствие требованиям стандартов (ГОСТ, СТР-К, ISO);
- определение наличия технических средств защиты информации на объекте информатизации;
- выявление организационно-распорядительной документации, регламентирующей защищенную обработку конфиденциальной информации.

По результатам данного этапа формируется отчет о состоянии защищенности объекта информатизации.

На этапе формирования модели угроз информационной безопасности формируется описание системы обработки информации, выявляются пользователи данной системы, определяется уровень исходной защищенности, степень актуальности угроз, рассчитывается вероятность реализации угроз.

Актуальность рисков определяется исходя из типа обрабатываемой информации, объема обрабатываемых в системе данных, структуры информационной системы, режима обработки данных и т.д.

Для того чтобы определить актуальность угроз для данного объекта информатизации, целесообразно выделить критерии актуальности каждой конкретной угрозы. Так, для угрозы сетевой атаки можно выделить такие критерии актуальности, как наличие доступа к глобальной сети, наличие в структуре локальной вычислительной сети средств межсетевого экранирования, антивирусной защиты и т.д.

Следующим этапом является формирование рекомендаций по совершенствованию системы защиты информации. Рекомендации разделяются на 3 основных раздела:

- рекомендации по организационной защите информации;
- рекомендации по инженерно-технической защите информации;
- рекомендации по программно-аппаратной защите информации.

По каждому разделу приводится ряд мер, выполнение которых необходимо для

защиты от выявленных угроз. Также на данном этапе подбираются оптимальные средства технической и программно-аппаратной защиты информации исходя из допустимой стоимости и набора необходимых характеристик.

Заключительным этапом является формирование организационно-распорядительной документации, регламентирующей защиту конфиденциальной информации.

На данном этапе проводится проверка наличия организационно-распорядительной документации на объекте, выявляются недостающие документы и, если нужно, проводится сбор данных, необходимых для формирования дополнительных документов.

Выходными данными этого блока является комплект организационно-распорядительной документации, регламентирующей защиту конфиденциальной информации.

Результаты работы автоматизированной системы представлены на рис. 2.

Рис. 2. Результаты работы автоматизированной системы оценки эффективности КСЗИ

Таким образом, на выходе автоматизированной системы формируется комплект документов, включающий модель угроз информационной безопасности рассматриваемого объекта, комплект организационно-распорядительной документации, регулирующей защиту конфиденциальной информации, и рекомендации по усовершенствованию системы защиты информации.

Поведение сложных информационных систем, подверженных внешним и внутренним деструктивным воздействиям, является неоднородным стохастическим процессом. С целью получения информации о динамике многомерной задачи требуется определить критерии, в соответствии с которыми будет осуществляться выбор инструмента математического моделирования.

Требования к математической модели включают возможности:

- учета вероятностей реализации и предотвращения угроз;
- моделирования процессов защиты во времени;

- моделирования одновременной реализации угроз во времени;

- учета своевременности реагирования средств защиты на угрозы безопасности.

Анализ данных критериев показал, что наиболее подходящим инструментом для моделирования процессов защиты информации является математический аппарат раскрашенных, вероятностных, ингибиторных сетей Петри.

Раскрашенные сети позволяют разделить фишки угроз безопасности и методов противодействия.

Вероятностные сети позволяют настроить вероятность совершения переходов (возникновение угроз и реагирование методов противодействия).

*Ингибиторные сети*позволяют реализовать процесс предотвращения угрозы безопасности методом противодействия.

Предлагается способ формального задания математической модели[8], построенной на базе ингибиторных, вероятностных и раскрашенных сетей Петри: сеть определяется как $F=<P,T,I,O>$, где $P=\{p1, p2, p3, p4, p5, p5'\}$ ($p1$ – возникновение источника угрозы, $p2$ – возникновение угрозы безопасности, $p3$ – прохождение угрозы через уязвимое звено, $p4$ - возникновение метода противодействия, $p5$ –деструктивное действие, $p5'$ – предотвращение угрозы безопасности); $T=\{t1,t2,t3,t3'\}$ – множество переходов; I – входные позиции; O - выходные позиции.

Для моделирования реагирования средств защиты на угрозы безопасности фишки в данной сети определены в множестве $color=\{red, blue\}$, причем фишки $color=red$ соответствуют угрозам безопасности, а фишки $color=blue$ - методам противодействия. При этом в позициях $\{p1, p2, p3, p5\}$ могут находиться только фишки $color=red$, в $\{p4, p5'\}$ - только фишки типа $color=blue$.

Для записи в формализованном виде каждого из способов срабатывания перехода $T=\{t1,t2,t3,t3'\}$ введем дополнительные операнды и параметры:

$F(p_i)$ – функция, отражающая наличие фишки в позиции p_i;

$\varphi(P)$ – функция, отражающая совершение/отражение угрозы с вероятностью P;

P_{threat} – вероятность совершения угрозы;

$P_{reaction}$ – вероятность устранения угрозы.

Правила срабатывания задаются с помощью терминальных языков[6] описания сетей Петри:

$P1^i \rightarrow \tau_i = t1^i(F_{P1i}),\ t2^i(F_{P2i},\ \varphi(P_{threat(n)})),\ t3^i(F_{P3i},\ ,\ \varphi(P_{reaction(m)},\ t3'^i(F_{P3i},\ \varphi(P_{reaction(m)}) \rightarrow P5^i,\ P5'^i$.

На основе исходных данных по рассматриваемому защищаемому объекту моделирования строится сеть Петри, фрагмент которой представлен на рис. 3.

Данная сеть является раскрашенной, вероятностной и ингибиторной [7], что позволяет реализовать следующие возможности:

1) вероятностная сеть позволяет учесть как средства нападения, так и средства отражения угроз безопасности за счет настройки вероятности совершения переходов;

2) раскрашенная сеть Петри позволяет идентифицировать фишки, ассоциируемые с угрозами безопасности и методами противодействия;

3) ингибиторная сеть Петри обеспечивает реализацию механизма предотвращения угроз безопасности методами противодействия.

Для разграничения действий злоумышленника и средств защиты в сети Петри представлены фишки двух типов: фишки типа *color=blue* – это фишки методов противодействия, а фишки типа *color=red* – это угрозы безопасности. Варианты развития событий изображены на рис. 4.

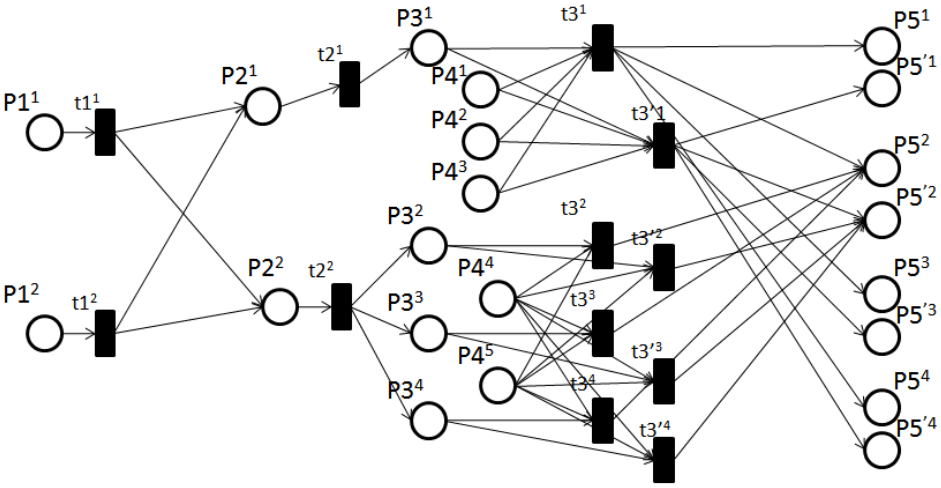

Рис. 3. Фрагмент построенной сети Петри

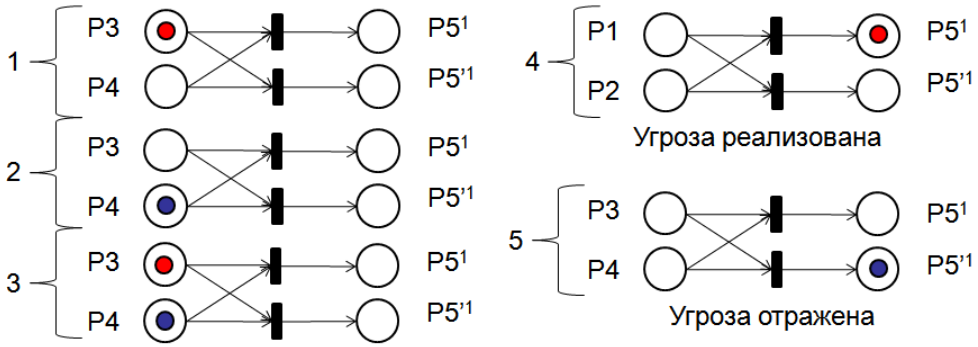

Рис. 4. Варианты развития событий

В первом случае (рис. 4) показана ситуация, когда существует угроза, а соответствующий ей метод противодействия пока не активен. В таком случае в следующий момент времени фишка красного цвета из позиции p3 попадает в позицию $p5^1$, что свидетельствует о реализации угрозы безопасности.

Во втором случае (рис. 4) показаны условия, когда метод противодействия готов к отражению угрозы. Самой угрозы пока не возникло, т.е. в позиции p3 фишка типа *red* отсутствует. А в позиции p4 находится фишка типа *blue*, что свидетельствует о том, что метод противодействия готов отразить угрозу с расчетной вероятностью предотвращения угрозы методом противодействия.

В третьем случае (рис. 4) рассмотрена предпосылка для реализации угрозы: в позиции p3 находится красная фишка. Также в позиции p4 находится синяя фишка – метод противодействия соответствующей угрозе. В следующий момент времени, по правилам работы ингибиторных сетей Петри, в соответствии с рассчитанной вероятностью отражения угрозы методом противодействия произойдет одно из двух возможных событий: реализация угрозы (фишка красного цвета переместится в позицию $p5^1$) либо успешное отражение угрозы (фишка синего цвета попадет в позицию $p5^2$).

Отличительной особенностью данной сети (рис. 3) является то, что она позволяет учитывать как действия угроз, так и действия средств защиты. Это обеспечивается тем, что переходы t2 данной сети настраиваются в соответствии с вероятностью совершения угрозы, а переходы t3 - в соответствии с расчетной вероятностью предотвращения угрозы методом противодействия. Это способствует более глубокому исследованию процессов защиты информации.

Далее для оценки эффективности моделируемой комплексной системы защиты информации предлагается использовать

специально разработанную весовую функцию.

В основе весовой функции лежит ряд критериев, отражающих вероятности совершения и отражения угрозы, а также степень опасности угрозы. Данная весовая функция будет накапливаться при отражении каждой угрозы, тем самым показывая эффективность системы защиты информации.

Предлагается рассчитать весовую функцию для каждой выявленной угрозы и присвоить расчетные значения переходам, соответствующим отражению угрозы t3'. Таким образом, суммарное значение весовой функции накапливается каждый раз, когда происходит событие ликвидации какой-либо угрозы (вариант 5 на рис. 4). Данный критерий отличается тем, что основывается на результатах моделирования угроз безопасности, т.е. отражает динамическое состояние СЗИ.

В результате анализа работ в области защиты информации обоснована формула для расчета весовой функции при ликвидации воздействия *i*-й угрозы:

$$W = \frac{P_{threat} + q_i^{threat} + (1 - P_{reaction})}{3};$$

$$\in [0,1],$$

где P_{threat} - вероятность совершения угрозы; $P_{reaction}$ - вероятность предотвращения угрозы; q_i^{threat} - коэффициент опасности угрозы.

Так как настоящее исследование опирается на нормативно-правовые акты ФСТЭК и ФСБ России, то для расчета вероятности совершения угрозы безопасности P_{threat} используется «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК. Исходя из данной методики вероятность совершения угрозы будет определяться соотношением

$$P_{threat} = Y_1 + Y_2 / 20,$$

где Y_1 - степень исходной защищенности; Y_2 - вероятность реализации угрозы.

В рамках рассматриваемой проблемы для расчета вероятности устранения угрозы безопасности $P_{reaction}$ предлагается применить методику, предложенную В.В. Домаревым, которая позволяет учитывать количественные и качественные требования по предотвращению угроз безопасности, а также их важность. Она заключается в том, что вероятность устранения угрозы безопасности представляется в виде функциональной зависимости

$$P_{reaction}(x_1 \ldots x_m) = \sum_{i=1}^{k} \omega_i \cdot \bar{x}_i + \sum_{i=k+1}^{m} \omega_i \cdot \mu(x_i),$$

где $\bar{x}_i$ - количественные требования к КСЗИ; ω_i - вес *i*-го требования; $\mu(x_i)$ - качественные требования к КСЗИ; k - число количественных требований; m - число качественных требований.

Предлагаемый подход к оценке уровня информационной безопасности объекта информатизации позволяет значительно сократить материальные и временные затраты на проведение аудита информационной безопасности, а также повысить качество проектных решений при создании и внедрении комплексных систем защиты информации.

Математический аппарат раскрашенных, вероятностных, ингибиторных сетей Петри позволяет оценить эффективность системы защиты объекта с учетом своевременности реагирования средств противодействия и одновременности реализации угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Рытов, М.Ю. Авторизация пользователей на основе комплексного применения методов распознавания лиц / М.Ю.Рытов, В.А.Шкаберин, Д.А.Лысов, А.П.Горлов // Информация и безопасность. - 2016. - №1. - С. 106-109.
2. Аверченков, В.И. Организационная защита информации/ В.И.Аверченков, М.Ю.Рытов. -

Брянск: БГТУ, 2010. - 184 с. - (Серия «Организация и технология защиты информации»).
3. Аверченков, В.И. Аудит информационной безопасности/ В.И.Аверченков. - Брянск: БГТУ, 2010. - 210 с. - (Серия «Организация и технология защиты информации»).
4. Аверченков, В.И. Автоматизация проектирования комплексных систем защиты информации: монография/ В.И.Аверченков, М.Ю.Рытов. - Брянск: БГТУ, 2012. - 147 с. - (Серия «Организация и технология защиты информации»).
5. Аверченков, В.И. Разработка системы технической защиты информации/ В.И.Аверченков, М.Ю.Рытов, А.В.Кувыклин, Т.Р.Гайнулин. - Брянск: БГТУ, 2008. - 187 с. - (Серия «Организация и технология защиты информации»).
6. Хопкрофт, Дж. Введение в теорию автоматов, языков и вычислений/ Дж.Хопкрофт, Р.Мотвани, Дж.Ульман. - М.: Вильямс, 2002. - 528 с.
7. Питерсон, Дж. Теория сетей Петри и моделирование систем/ Дж.Питерсон. - М.: Мир, 1984. - 264 с.
8. Пентус, А. Е. Математическая теория формальных языков/ А.Е.Пентус. - М.: Интернет-ун-т информ. технологий: БИНОМ. Лаборатория знаний, 2006. - 248 с.

1. Rytov, M.Yu. User authorization based on complex application of methods for persons identification / M.Yu.Rytov, V.A.Shkaberin, D.A.Lysov, A.P.Gorlov // *Information & Security.* - 2016. - №1. - pp. 106-109.
2. Averchenkov, V.I. Information organization protection/ V.I. Averchenkov, M.Yu.Rytov. - Bryansk: BSTU, 2010. – pp. 184. - (*Series "Organization and Techniques for Information Protection"*).
3. Averchenkov, V.I. Information Security Audit/ V.I.Averchenkov. - Bryansk: BSTU, 2010. – pp. 210. - (*Series "Organization and Techniques for Information Protection"*).
4. Averchenkov, V.I. Computer-aided design of complex systems for information protection: monograph/ V.I.Averchenkov, M.Yu.Rytov. - Bryansk: BSTU, 2012. – pp. 147. - (*Series "Organization and Techniques for Information Protection"*).
5. Averchenkov, V.I. System development for information engineering protection / V.I.Averchenkov, M.Yu.Rytov, A.V.Kuvyklin, T.R.Gainulin. - Bryansk: BSTU, 2008. – pp. 187. - (*Series "Organization and Techniques for Information Protection"*).
6. Hopkroft, J. *Introduction to the Theory of Automatic Units, Languages and Computations*/ J.Hopkroft, R.Motvani, J.Ulman. - M.: Williams, 2002. – pp. 528.
7. Peterson, J. *Theory of Petri Nets and Systems Modeling*/ J.Peterson. - M.: World, 1984. – pp. 264.
8. Pentus, A. E. Mathematical Theory of formal languages/ A.E.Pentus. - M.: *Internet-University of Information Techniques: BINOM. Knowledge Laboratory*, 2006. – pp. 248.

Статья поступила в редколлегию 24.02.2016.
Рецензент: д.т.н., профессор Брянского государственного технического университета Аверченков В.И.

Сведения об авторах:

Рытов Михаил Юрьевич, к.т.н., доцент, зав. кафедрой «Системы информационной безопасности» Брянского государственного технического университета, e-mail: rmy@tu-bryansk.ru.
Горлов Алексей Петрович, аспирант кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: apgorlov@gmail.com.
Лысов Дмитрий Андреевич, студент кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: lysovdmitriia@gmail.com.

Rytov Mikhail Yurievich, Can.Eng., Assistant Prof., Head of the Dep. "Information Security Systems", Bryansk State Technical University, e-mail: rmy@tu-bryansk.ru.
Gorlov Alexey Petrovich, Post graduate student of the Dep. "Information Security Systems", Bryansk State Technical University, e-mail: apgorlov@gmail.com.
Lysov Dmitry Andreevich, Student of the Dep. "Information Security Systems", Bryansk State Technical University, e-mail: lysovdmitriia@gmail.com.