УДК 347.775
DOI: 10.12737/article_5a337fbde60ab3.69866796

В.Т. Еременко, М.Ю. Рытов, А.П. Горлов, В.И. Аверченков, В.П. Фёдоров

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

Рассмотрено моделирование 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 информатизации, защищенность, аппарат сетей Петри.

V.T. Eremenko, M.Yu. Rytov, A.P. Gorlov, V.I. Averchenkov, V.P. Fyodorov

EFFICIENCY ASSESSMENT PROCESS SIMULATION OF COMPLEX SYSTEMS FOR INFORMATION PROTECTION OF ENTERPRISES AT THREAT SIMULTANEOUS REALIZATION

The purpose of this paper is a thorough consideration of approaches to the process assessment simulation of the complex system efficiency for information protection of enterprises at the simultaneous realization of some threats. On the statistics basis during recent years in the statistics there is substantiated a topicality of subjects chosen, basic problems of data protection are described. Basic regulations used at the formation of a complex system for information protection are presented. A process for the development of simulators, information support and a software complex for an automation assessment of the protection level and complex system efficiency of information protection is described. The paper reports the circuit of the operation mechanism of the automated system for the efficiency assessment of the information protection system used at an enterprise, and also basic results of the application of a similar software complex: documentation, simulators of potential threats, recommendations for protection system updating are considered. Petri network is formed on the basis of initial data on the considered protected object of modeling. It is colored, probable and inhibitory which allows assessing the efficiency of the system of object protection taking into account timeliness of the reaction of counteraction means and threat realization simultaneity. The conclusions on the efficiency of use of the procedure presented are drawn.

Key words: information security, efficiency assessment, IF audit, threat model, automated system, informatization object, security, apparatus of Petri network.

Введение

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

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 [1; 2].

Комплексная система защиты информации (КСЗИ) - это система, в которой действуют в единой совокупности правовые, организационные, технические, программно-аппаратные и другие подсистемы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки. Составные элементы КСЗИ: 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.

Методика оценки защищенности объекта информатизации

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 [2; 4].

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 (автоматизированной системы) 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 включает (рис. 1):

1. Ввод исходных данных.
2. Формирование информационной модели объекта информатизации.
3. Оценку состояния защищенности ОИ.
4. Математическое моделирование угроз ИБ.
5. Формирование модели угроз ИБ.
6. Формирование рекомендаций по совершенствованию системы защиты информации.
7. Формирование организационно-распорядительной документации. 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 оценивать еще на этапе проектирования целесообразность использования той или иной СЗИ, а также моделировать взаимодействие СЗИ в едином информационном пространстве [3].

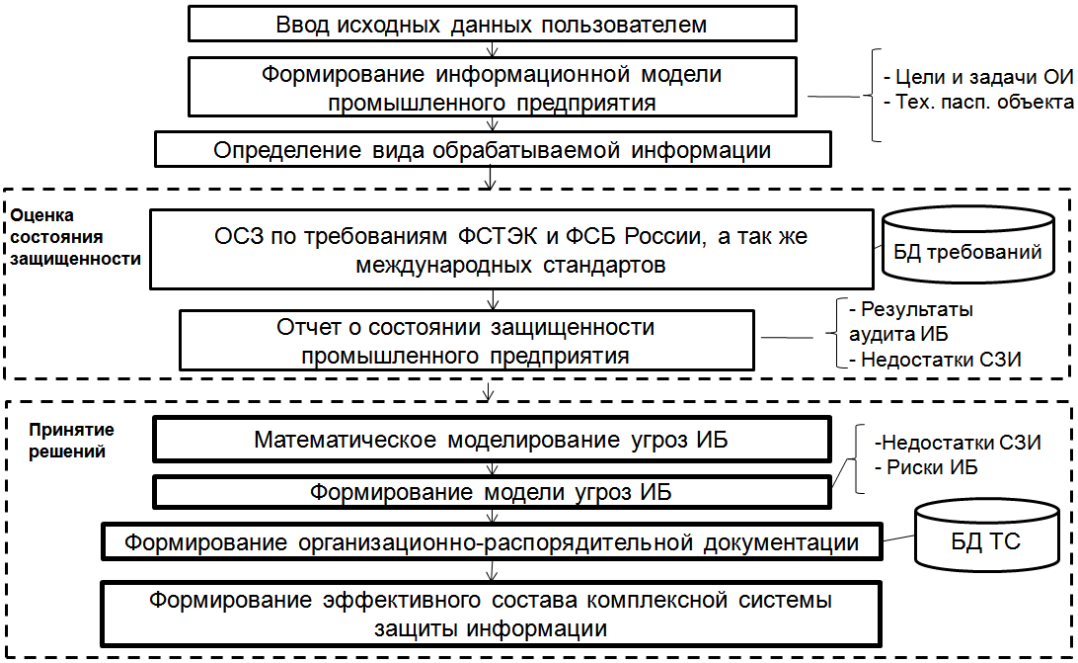

Рис. 1. Механизм работы АС оценки эффективности КСЗИ

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 [5].

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 АС оценки эффективности КСЗИ

Модель реагирования средств защиты на угрозы безопасности

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 [5] 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.

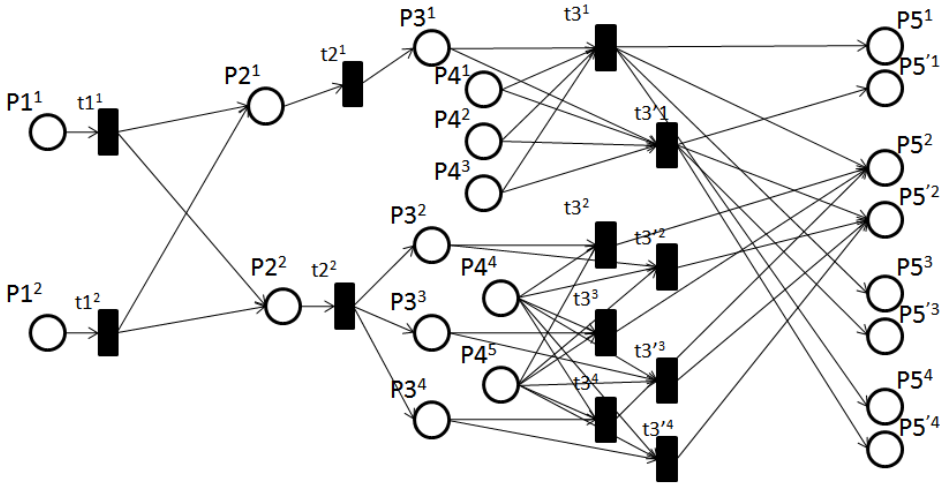

Рис. 3. Фрагмент построенной сети Петри

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

1) вероятностная сеть позволяет учесть как средства нападения, так и средства отражения угроз безопасности за счет настройки вероятностей 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 [6].

Заключение

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. Аверченков, В.И. Организационная защита информации / В.И. Аверченков, М.Ю. Рытов. - Брянск: БГТУ, 2010. - 184 с. - (Серия «Организация и технология защиты информации»).
2. Аверченков, В.И. Аудит информационной безопасности / В.И. Аверченков. - Брянск: БГТУ, 2010. - 210 с. - (Серия «Организация и технология защиты информации»).
3. 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»).
4. 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»).
5. Хопкрофт, Дж. Введение в теорию автоматов, языков и вычислений / Дж. Хопкрофт, Р. Мотвани, Дж. Ульман. - М.: Вильямс, 2002 . - 528 с.
6. Питерсон, Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. - М.: Мир, 1984. - 264 с.

1. Averchenkov, V.I. Organizational protection of information / V.I. Averchenkov, M.Yu. Rytov. – Bryansk: BSTU, 2010. – pp. 184. - (*Series "Organization and Techniques for Information Protection"*).
2. Averchenkov, V.I. Audit of information safety / V.I. Averchenkov. – Bryansk: BSTU, 2010. – pp. 210. - (*Series "Organization and Techniques of Information Protection"*).
3. Averchenkov, V.I. Design automation 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"*).
4. Averchenkov, V.I. Development of Technical Information Protection System / V.I. Averchenkov, M.Yu. Rytov, A.V. Kuvyklin, T.R. Gainulin. – Bryansk: BSTU, 2008. – pp. 187. – (*Series "Organization and Techniques for Information Protection"*).
5. Hopcroft, J. *Introduction into Theory of Automatic Machines, Languages and Computations* / J. Hopcroft, R. Motvani, J. Ulman. – M.: Williams, 2002. – pp. 528.
6. Peterson, J. *Petri Network Theory and System Modeling* / J. Peterson. – M.:World, 1984. – pp. 264.

Статья поступила в редколлегию 20.11.17.
Рецензент: д.т.н., профессор Брянского государственного технического университета Горленко О.А.

Сведения об авторах:

Еременко Владимир Тарасович, д.т.н., профессор, зав. кафедрой «Информационная безопасность» Орловского государственного университета им. И.С. Тургенева, Тел.: +7(920)812-65-64, e-mail: wladimir@orel.ru.

Горлов Алексей Петрович, к.т.н., доцент кафедры «Системы информационной безопасности» Брянского государственного технического университета, Тел.: +7(980)-302 -83 – 80 e-mail: apgorlov@gmail.com.

Аверченков Владимир Иванович, д.т.н., профессор кафедры «Компьютерные технологии и системы» Брянского государственного технического университета, тел.:(4832) 56-05-33, e-mail: aver@tu-bryansk.ru.

Рытов Михаил Юрьевич, к.т.н., доцент, заведующий кафедрой «Системы информационной безопасности» Брянского государственного технического университета, тел.: (4832) 51-13-77, e-mail: rmy@tu-bryansk.ru.

Фёдоров Владимир Павлович, д.т.н., профессор кафедры «Технология машиностроения» Брянского государственного технического университета, тел.: (4832) 58-82-20 e-mail: tm-bgtu@yandex.ru.

Eryomenko Vladimir Tarasovich, D. Eng., Prof. Head of the Dep. "Information Safety", Turgenev State University of Orel, e-mail: wladimir@orel.ru.

Gorlov Alexey Petrovich, Can. Eng., Assistant Prof. of the Dep. "Systems of Information Safety", Bryansk State Technical University, e-mail: apgorlov@gmail.com.

Averchenkov Vladimir Ivanovich, D. Eng., Prof. of the Dep. "Computer Technologies and Systems", Bryansk State Technical University, e-mail: aver@tu-bryansk.ru.

Rytov Mikhail Yurievich, Can. Eng., Assistant Prof., Head of the Dep. "Systems of Information Safety", Bryansk State Technical University, e-mail: rmy@tu-bryansk.ru.

Fyodorov Vladimir Pavlovich, D. Eng., Prof. of the Dep. "Engineering Techniques", Bryansk State Technical University, e-mail: tm-bgtu@yandex.ru.