УДК 004.056

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ ИНГИБИТОРНЫХ, ВЕРОЯТНОСТНЫХ И РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ ОТ УТЕЧКИ ИНФОРМАЦИИ

М.Ю. Рытов, В.Т. Еременко, А.П. Горлов

В статье рассматривается процесс автоматизации оценки состояния защищенности объекта информатизации, с применением аппарата ингибиторных, вероятностных и раскрашенных сетей Петри

Ключевые слова: информационная безопасность, оценка состояния защищенности, математическая модель, сети Петри

Комплексная система защиты информации - это система, в которой действуют в единой совокупности правовые, организационные, технические, программно-аппаратные и другие нормы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки. Элементы КСЗИ, в свою очередь, в общем виде, состоят из средств, устройств и способов защиты информации, а также методов их использования.

Понятие защиты информации в настоящее время ассоциируется, как правило, с проблемами обеспечения информационной безопасности в информационных системах (ИС).

Комплексная система защиты информации (КСЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых в ИС для решения в ней выбранных задач защиты. Задачи же защиты информации решаются с целью нейтрализации дестабилизирующего воздействия причин нарушения целостности информации при обеспечении физической целостности информации или с целью перекрытия каналов несанкционированного получения информации – при защите от несанкционированного получения информации.

Отсутствие на объектах информатизации систем защиты информации приводит к утечке конфиденциальной информации так как разработка и внедрение таких систем является достаточно затратной процедурой. Автоматизированная система оценки уровня ИБ позволит привести систему ОИ в соответствие установленным требованиям, противостоять актуальным угрозам, снизить трудоемкость работ, сэкономить время и значительно сократить материальные затраты на проведение аудита и разработку СЗИ [1,2].

Ввиду этого разработка системы автоматизированной оценки уровня информационной безопасности объекта информатизации представляется актуальной.

В большинстве своем существует практика создания единой системы защиты из существующих разрозненных элементов, где к уже существующей информационной среде добавляются средства защиты информации. Современные условия диктуют другой подход, который заключается в том, что изначально вся информационная среда 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 их взаимодействие в едином информационном пространстве.

Состав и функциональность проектируемой СЗИ должны соответствовать актуальным для

Рытов Михаил Юрьевич – БГТУ, канд. техн. наук, доцент, (4832)56-24-08

Еременко Владимир Тарасович – БГТУ, д-р техн. наук, профессор, (4832)56-24-08

Горлов Алексей Петрович – БГТУ, аспирант, (4832)56-24-08

рассматриваемой информационной системы угрозам. Для обеспечения этого требования необходимо на этапе проектирования выявить существующие уязвимости и угрозы информационной безопасности, определить степень актуальности этих угроз и вероятность их реализации, а так же 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 [3].

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

На рис.1 этот процесс представлен блоком оценки состояния защищенности. На данном этапе на основе результатов оценки соответствия требованиям нормативно-правовой базы требуется выявить уязвимости информационной системы.

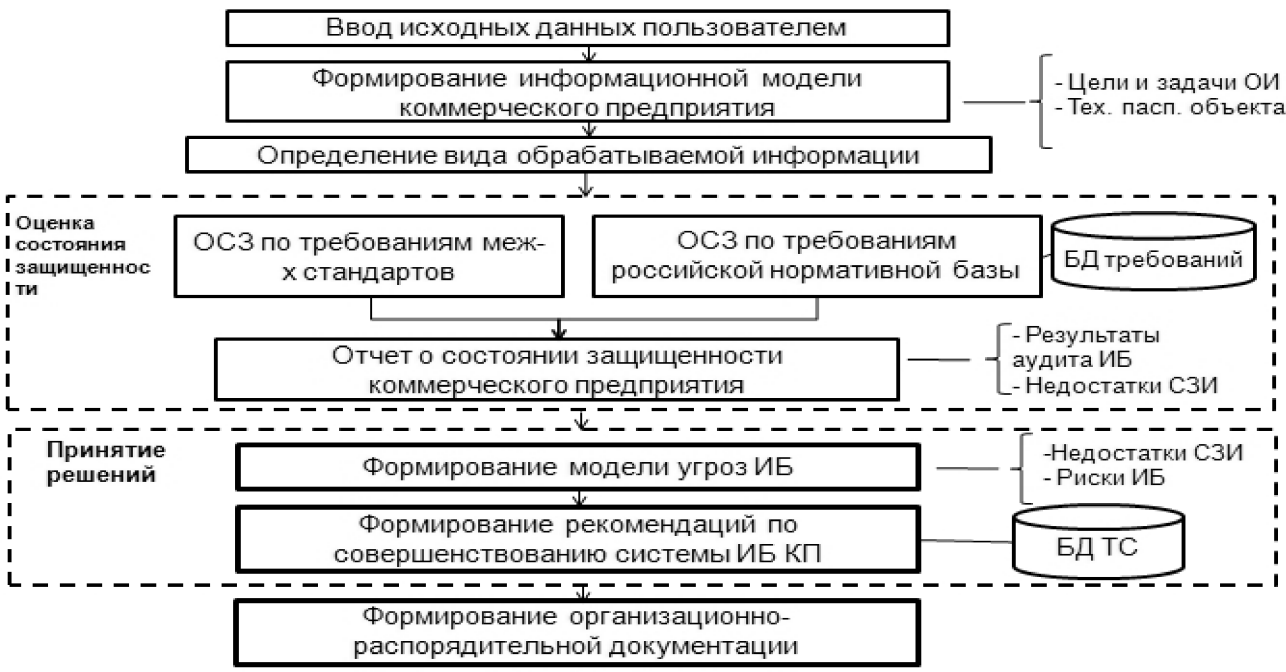

Рис. 1. Алгоритм работы автоматизированной системы.

На предыдущем этапе работы системы был сформирован информационный портрет объекта информатизации который позволяет определить объекты и субъекты информационной безопасности, другими словами определяется информация подлежащая защите.

Для моделирования СЗИ было принято решение использовать раскрашенные, вероятностные и ингибиторные сети Петри [4]. Обоснованность применения таких сетей представлена в таблице 1.

Таблица 1. Подклассы сетей Петри

Раскрашенные	позволяют «разделить» фишки угроз безопасности и методов противодействия
Вероятностные	позволяют настроить вероятность совершения переходов: возникновение угроз и реагирования методов противодействия
Ингибиторные	позволяют реализовать процесс предотвращения угрозы безопасности методом противодействия

Предлагается способ формального задания математической модели, построенной на базе ингибиторных, вероятностных и раскрашенных сетей Петри: $F =< P,T,I,O >$, 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, $p5$ – нанесение деструктивного действия, $p5'$ – предотвращение угрозы безопасности, $T = \{t1, t2, t3\}$ – множество переходов, I – входные позиции, O – выходные позиции. Для моделирования своевременности реагирования средств защиты на угрозы безопасности фишки в данной сети определены на множестве $Color = \{red, blue\}$, причем фишки $Color = red$ ассоциируются с угрозами безопасности, а фишки $Color = blue$ с методами противодействия. При этом в позициях $\{p1, p2, p3\}$ могут находиться только фишки $Color = red$, $\{p4\}$ – только фишки типа $Color = blue$, а в позициях $\{p5, p5'\}$ как те, так и другие.

Для записи в формализованном виде каждого из способов срабатывания перехода $T = \{t1, t2, t3\}$, введем дополнительные операнды и параметры:

$Q(p^i)$ – отражает наличие фишки в позиции *i*;

$\varphi(T,t)$ – отражает вероятность совершения перехода T;

$++(p^i, C, \varphi)$ – увеличивает количество фишек цвета C с вероятностью φ в позиции *p* на 1;

$--(p^i, C, \varphi)$ – уменьшающий количество фишек цвета C с вероятностью φ в позиции p^i на 1;

$Time$ – время моделирования в тактах;

P_{threat} – вероятность совершения угрозы;

$P_{reaction}$ – вероятность устранения угрозы;

$Y(p3^i, p4^j, t3^h)$ - возвращает 1, если позиции $p3^i$ и $p4^j$ связаны с переходом $t3^h$.

Используя продукционные правила, которые успешно применяются для описания логики работы системы, представим правило срабатывания перехода $t1$:

$$\forall t \in t1^i (Input(p1^i, t1^i, t, \mu)) \Rightarrow$$
$$AddSort(TR, t, 1))$$
$$\forall t \in TR(Max(TR, t)) \Rightarrow$$
$$I(p1^i, t1^i, \mu) O(p2^i, t1^i, \mu) Rem(TR, t).$$

Перехода $t2$:

$$\forall t \in t2^i (Input(p2^i, t2^i, t, \mu)) \Rightarrow$$
$$AddSort(TR, t, \varphi(t2^i, t))$$
$$\forall t \in TR(Max(TR, t)) \Rightarrow$$
$$I(p2^i, t2^i, \mu) O(p3^i, t2^i, \mu) Rem(TR, t)$$

, где

$$\varphi(t2^i, t) = P^i_{threat}$$

Перехода $t3$:

$$((\forall t \in TR(Max(TR, t))) \cap (Y(p3^i, p4^k, t3^h) = 1) \Rightarrow$$
$$I(p3^i, p4^k, t, \mu) O(p5'^m, t, \mu) Rem(TR, t) \cap$$
$$\cap (W = W + W(t3^h, t)) \cap (++(p5'^m, blue, 1))) \cup$$
$$((\forall t \in TR(Max(TR, t))) \cap (Y(p3^i, p4^k, t3^h) = 0) \Rightarrow$$
$$I(p3^i, p4^k, t, \mu) O(p5'^m, t, \mu) (Rem(TR, t)) \cap$$
$$(++(p5^i, red, 1)));$$

Фрагмент сети Петри (цветная, ингибиторная, вероятностная), используемой для выявления уязвимостей СЗИ и угроз представлен на рис. 2:

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.

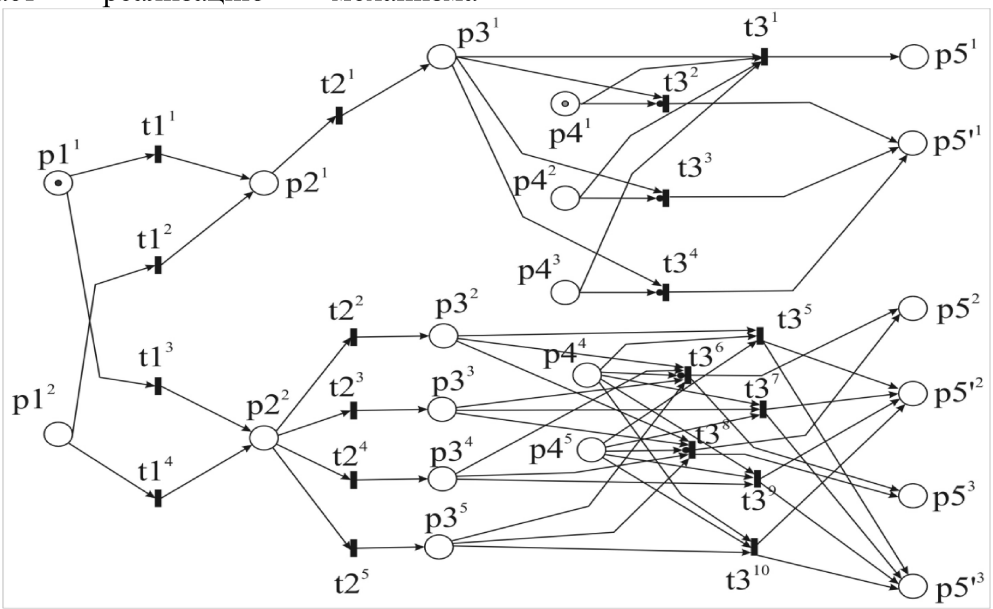

Рис.2. Фрагмент сети Петри, используемой для оценки состояния защищенности.

Таким образом, использование ингибиторных, вероятностных и раскрашенных сетей Петри позволяет оценить состояние защищенности объекта информатизации от утечки информации, а так же учесть одновременность совершения атак и своевременность противодействия защитных механизмов.

Литература

1. 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»).

2. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р., Рудановский М.В. Проектирование политики безопасности информационных технологий на основе методов когнитивного моделирования/ Вестник БГТУ, № 3, 2011 г. С.118-125.

3. Гришина, Н.В. Организация комплексной системы защиты информации/ Н.В. Гришина. - М.: Гелиос АРВ, 2007. -256 с.

4. Питерсон Дж. Теория сетей Петри и моделирование систем. — М: Мир, 1984. — 264 с.

5. Котов В. Е. Сети Петри. — М: Наука, 1984. — 160 с.

ФГБОУ ВПО «Брянский государственный технический университет»
Bryansk state technical university

AUTOMATION ASSESSMENT PROCESS PROTECTED WITH INHIBITORY, PROBABILISTIC AND COLOURED PETRI NETS

M.U. Rytov, V.T. Eremenko, A.P. Gorlov

The article deals with the process automation facility security assessment of information, using the apparatus of the inhibitor, and the probability of colored Petri nets

Key words: information security, security assessment, mathematical model, Petri nets