ДЕПАРТАМЕНТ СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ ВОРОНЕЖСКОЙ ОБЛАСТИ

пл. Ленина, 1, г. Воронеж, 394018
Телефон (473) 212-65-05, факс (473) 212-65-22,
e-mail: dsmk@govvrn.ru

Руководителю
(по списку)

08.06.2015 № 42-11/480

На № от

О проведении Международной научно-практической конференции

В период с 20 по 21 августа 2015 года в г. Воронеже запланировано проведение V Воронежского форума инфокоммуникационных и цифровых технологий, включающего международную научно-практическую конференцию «Обеспечение безопасности инфокоммуникационных и цифровых технологий».

Прошу Вас поддержать инициативу проведения V Воронежского форума инфокоммуникационных и цифровых технологий принятием участия в организационном комитете указанной конференции. Также прошу рассмотреть вопрос подготовки докладов по вышеуказанной тематике с возможностью дальнейшей публикации в журнале из перечня ВАК и направления представителей ВУЗа для участия в научно-практической конференции «Обеспечение безопасности инфокоммуникационных и цифровых технологий».

Информацию прошу направить в департамент в срок до 22.06.2015 на адрес электронной почты: apotapov@govvrn.ru.

Приложение: на 10 л. в 1 экз.

Руководитель департамента А.Ю. Верховцев

Потапов
212-65-02

Приложение 1

V Воронежский форум инфокоммуникационных и цифровых технологий»

Концепция Международной научно-практической конференция «Обеспечение безопасности инфокоммуникационных и цифровых технологий».

Название проекта:
V Воронежский форум инфокоммуникационных и цифровых технологий
Дата проведения:
20 августа 2015 года

В указанная конференция планируется провести в следующем составе:

Научное руководство:

Борисов Василий Иванович - член-корреспондент РАН, научный руководитель ОАО «Концерн «Созвездие».

Новиков Дмитрий Александрович - член-корреспондент РАН, заместитель директора Института проблем управления им. В.А. Трапезникова РАН.

Руководство оргкомитета:

Петренко Владимир Романович - ректор Воронежского государственного технического университета.

Радько Николай Михайлович – заместитель генерального директора ОАО «Концерн «Созвездие».

Щербаков Владимир Борисович – начальник Государственного научно-исследовательского испытательного института проблем технической защиты информации ФСТЭК России.

Оргкомитет:

Алиев А.А. – заведующий кафедрой «Информационные технологии и программирование» Бакинского государственного университета. Громов Ю.Ю. – директор института автоматики и информационных технологий Тамбовского государственного технического университета. Зегжда П.Д. – заведующий кафедрой «Информационная безопасность компьютерных систем» Санкт-Петербургского государственного технического университета. Калашников А.О. – ведущий научный сотрудник Института проблем управления им. В.А. Трапезникова РАН. Кравец О.Я. – директор издательства «Научная книга». Лось В.П. – проректор по научной работе Московского государственного университета приборостроения и информатики. Львович И.Я. – ректор Воронежского института высоких технологий. Остапенко Г.А. – начальник отдела защиты информации и связи департамента связи и массовых

коммуникаций Воронежской области. Поваляев А.Д. – проректор по научной работе и зарубежным связям Воронежского государственного технического университета. Ружицкий Е. – декан факультета информатики Пан-Европейского университета. Самигулина Г.А. – заведующая лабораторией «Интеллектуальные системы управления и прогнозирования» Института информационных и вычислительных технологий Комитета науки Министерства образования и науки Республики Казахстан. Тарасов А.А. – директор института информационных наук и безопасности Российского государственного гуманитарного университета. Чернобров П. – директор компании Host-Telecom.

Секретариат:

Бурса Максим Васильевич - ассистент кафедры систем информационной безопасности Воронежского государственного технического университета.

Остапенко Александр Григорьевич - руководитель Регионального учебно-научного центра по проблемам информационной безопасности.

Плотников Денис Геннадьевич - старший преподаватель кафедры систем информационной безопасности Воронежского государственного технического университета.

Программа проведения V Воронежского форума

Регламент: обычный доклад - до 7 мин; перерыв - через каждые 1,5 часа.

Доклады участников конференции, представляющих следующие организации:

Зарубежные вузы и фирмы (состав уточняется). Академия ФСО России. Астраханский государственный технический университет. Брянский государственный технический университет.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России. Институт проблем управления РАН. Казанский государственный технический университет им. А.Н. Туполева. Курский государственный университет. Московский инженерно-физический институт. Московский государственный технический университет им. Н.Э. Баумана. АО «Концерн «Созвездие». Оренбургский государственный технический университет. Пензенский государственный университет. Санкт-Петербургский государственный технический университет. Сыктывкарский государственный университет. Таганрогский технологический институт Южного федерального университета. Тамбовский государственный технический университет. Уфимский государственный авиационно-технический университет.

Международный институт компьютерных технологий. Воронежский государственный технический университет. Воронежский государственный университет. Воронежский институт МВД России. Воронежский институт правительственной связи ФСО России. Воронежский институт ФСИН России. Воронежский институт высоких технологий. Воронежский архитектурно-строительный университет, ВУНЦ ВВС «Военно-воздушная академия им. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

Оргвзнос не взимается

Рабочие языки конференции: русский и английский.

Примечание: материалы (желательно с зарубежным соавторством) в объеме четырех полных страниц по формату (www.kafedrasib.ru) журнала «Информация и безопасность» будут опубликованы в выпусках № 3 и 4 этого журнала, пятилетний импакт-фактор (без самоцитирования) которого составляет 3,039. Прием материалов осуществляется до 21 июня 2015 года.

Возможно заочное участие в конференции с последующим опубликованием представленных материалов.

Образец оформления материалов прилагается. Его несоблюдение может быть основанием для отказа в рассмотрении.

Приложение 2

Анкета участника (заявка)
Международной научно-практической конференции «Обеспечение безопасности инфокоммуникационных и цифровых технологий» (заполняется на отдельном листе)

1. Ф.И.О. участника (полностью)	
2. Дата рождения	
3. Место работы или учебы	
4. Структурное подразделение где работает участник (факультет, отделение, курс для учащихся)	
5. Домашний адрес	
6. E-mail	
7. Контактный телефон	
8. Ф.И.О. научного руководителя (полностью)	
9. Участие в конференции (очное/заочное)	
10. Необходимость размещения в гостинице*	
сколько требуется мест	
дата приезда	
дата отъезда	

*** Расходы, связанные с проездом, проживанием и питанием участника конференции оплачиваются за счет командирующей стороны.**

Приложение 3

Требования к оформлению тезисов доклада

Тезисы на русском языке приводятся в объеме не более 1 страницы формата А4, который содержит:

1. **УДК**.
2. **Заголовок тезисов**
3. ФИО полностью, ученая степень, ученое звание, место работы, должность, контактный телефон, адрес электронной почты
4. **Текст тезисов доклада**, кратко излагающий актуальность, научно-техническую новизну, отраслевую принадлежность, результаты, предложения по внедрению.
5. **Список источников не приводится**.

Требования к оформлению:

Тезисы набираются в текстовом редакторе Microsoft Word (или аналогичном) и оформляются в соответствии с требованиями: шрифт – Times New Roman, кегль (размер шрифта) – 14 пт., интервал – полуторный; поля: левое – 30 мм; верхнее и нижнее – 20 мм; правое – 15 мм.

==Поля==: Верхнее 2,35см; Нижнее 2,35см; Левое 2,5см; Правое 1,5см; ==Абзац== 0,8см; ==Междустрочный интервал== 1,0; ==Интервал перед и после абзаца должен отсутствовать== ==Колонки:== Ширина 8,25см Промежуток 0,5см; ==Рисунки, формулы, таблицы располагаются по центру==

Приложение 4

Образец оформления статьи

УДК 004.056.53

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

Рытов Михаил Юрьевич – БГТУ, канд. техн. наук, доцент, e-mail: rmy@tu-bryansk.ru

Еременко Владимир Тарасович - Государственный университет – учебно-научно-производственный комплекс, д-р техн. наук, профессор, e-mail: wladimir@orel.ru

Горлов Алексей Петрович – БГТУ, аспирант, e-mail:sib@tu-bryansk.ru

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 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 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 [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.

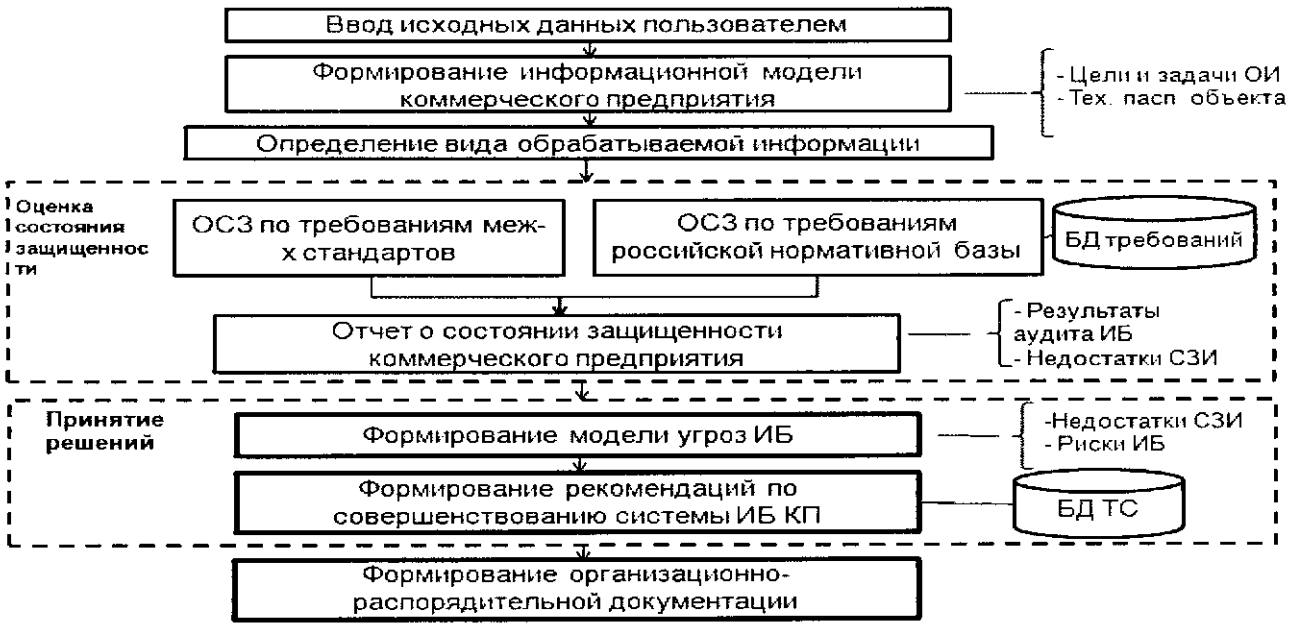

Рис. 1. Алгоритм работы автоматизированной системы

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 ниже.

Табл. 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.

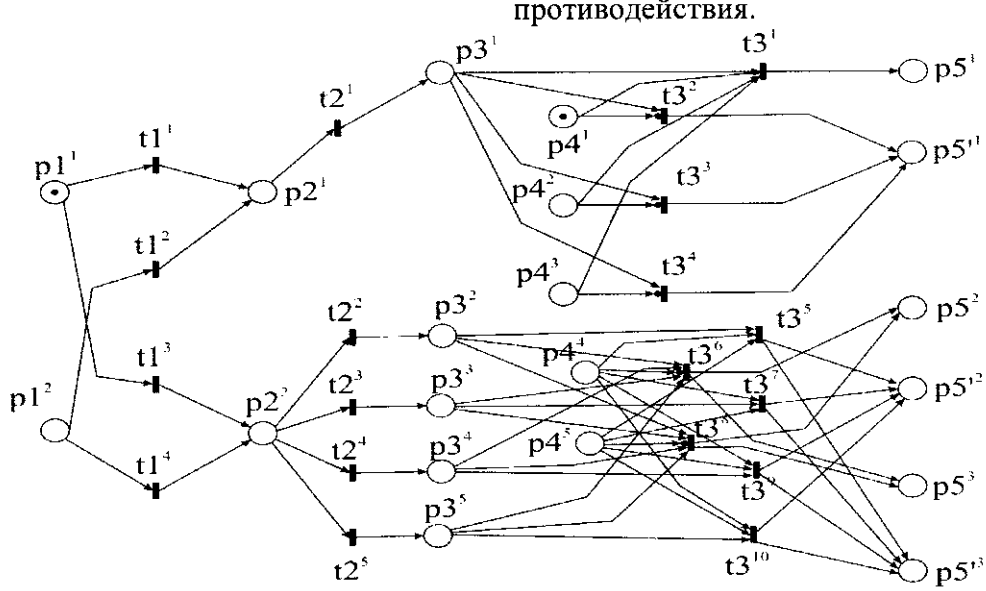

Рис. 2. Фрагмент сети Петри, используемой для оценки состояния защищенности

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

Литература

1. Разработка системы технической защиты информации [Текст] / 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. Проектирование политики безопасности информационных технологий на основе методов когнитивного моделирования [Текст] / Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р., Рудановский М.В. //Вестник БГТУ, № 3, 2011 г. С.118-125.

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

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

5. Котов, В. Е. [Текст] // 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