Цыбулин Анатолий Михайлович
Федеральное государственное бюджетне образовательное учреждение высшего профессионального образования «Волгоградский государственный университет».
E-mail: anatsybulin@yandex.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Зав. кафедрой информационной безопасности.

Tsybulin Anatoly Mihaylovich
Volgograd State University.
E-mail: anatsybulin@yandex.ru.
100, Universitetsky Pr., Volgograd, 400062, Russia.
Phone: +78442460368.
Head of Department of Information Security.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

СЕТИ ПЕТРИ КАК ИНСТРУМЕНТ АНАЛИЗА СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Построение системы защиты является обязательным условием для обеспечения безопасности конфиденциальной информации, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы является построение раскрашенных сетей Петри. С помощью аппарата сетей Петри проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Система защиты конфиденциальной информации; информационная система; сети Петри.

V.G. Mironova, A.A. Shelupanov

PETRI NETS AS A TOOL FOR THE ANALYSIS OF THE PROTECTION CONFIDENTIAL INFORMATION

Building security is a prerequisite for the security of confidential information stored and processed in the information system. System requirements of information security are formed based on the results of the survey and information system aimed at neutralizing the vulnerabilities of the system. One way of security analysis system is the construction of colored Petri nets. With the help of Petri nets functioning of the survey is conducted of the implemented system security and identify its weaknesses.

System to protect confidential information; information system; Petri net.

Развитие информационных систем обработки и хранения конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование информационной системы (ИС), в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности конфиденциальной информации (КИ), а также составляются требования к СЗКИ.

Требования к СЗКИ, в зависимости от вида КИ определяются согласно нормативно-законодательной базы Российской Федерации (РФ). Одним из видов КИ являются персональные данные (ПДн). Согласно Федеральному закону №152-ФЗ «О персональных данных» от 27 июля 2006 г., для всех информационных систем персональных данных (ИСПДн) должны быть построены СЗКИ [1]. При построении СЗКИ для ИСПДн необходимо руководствоваться Приказом № 58 «Об утверждении методов и способов защиты персональных данных, обрабатываемых в информационных системах персональных данных».

Воспользуемся аппаратом раскрашенных сетей Петри, как инструментом анализа СЗКИ, реализованной в системе. Требования к ИСПДн установлены в [2]. Сеть Петри представляет собой двудольный граф вида:

$$П = \{A, T, O_A(T), O_T(A)\},$$

где А – множество позиций сети Петри, моделирующих состояние рассматриваемого процесса;

Т – множество переходов сети Петри, моделирующих условия перехода из состояние в состояние;

$O_A(T)$ – входная функция переходов (выходная функция позиций), отражающая множество А в множество Т;

$O_T(A)$ – входная функция переходов (выходная функция позиций), отражающая множество Т в множество А [3].

Существует несколько видов сетей Петри:

- временные сети – для учета временных характеристик;
- раскрашенные сети – интерпретация реальных систем.

Однако в раскрашенных сетях не допускается представление эффектов размножения и синхронизации. Меткам раскрашенной сети Петри приписывают атрибуты, которые называют цветами. Правила возбуждения переходов дополняются условиями, предполагающими выбор меток определенных цветов. Для описания процессов обработки ПДн в ИСПДн и формирования требований к СЗКИ будем использовать аппарат раскрашенных сетей Петри.

Пусть в ИСПДн №1 обрабатываются сведения о фамилии, имени, отчестве, адресе места жительства сотрудника, объем ПДн не превышает 1000 записей. Согласно [4], ПДн, обрабатываемые в ИСПДн №1 относятся к 3-й категории и 3-му объему, поэтому ИСПДн №1 присвоен класс 3.

ИСПДн №1 имеет следующие характеристики: автономная, однопользовательская, без разграничения прав доступа, без возможности подключения к сети связи общего пользования, ИСПДн находится на территории РФ.

Идентификация пользователя при входе в ИСПДн №1 производится по паролю, требований к которому в организации не установлено. Регистрация пользователя при входе (выходе) в систему (из системы) производится по идентификатору пользователя, однако регистрация загрузки и инициализации операционной системы и ее программного останова не производится.

Пользователь осуществляет ввод/изменение данных в ИСПДн №1.

На рис. 1 представлена блок-схема алгоритма и сеть Петри входа пользователя в ИСПДн №1 и используются следующие обозначения:

pass – пароль, введенный пользователем для аутентификации (фишка типа 1 – правильный пароль, который соответствует всем требованиям; фишки другого типа – неправильные и (или) некорректные пароли);

iden – идентификатор, который использует пользователь для идентификации в системе (фишка типа 2 – идентификатор корректен и удовлетворяет всем условиям; фишки другого типа – неправильные и (или) некорректные идентификаторы);

a1 – пароль введен пользователем в окно запроса пароля;

a2 – идентификатор введен пользователем;

a3 – предъявленный идентификатор подтвержден введенным паролем, аутентификация прошла успешно;

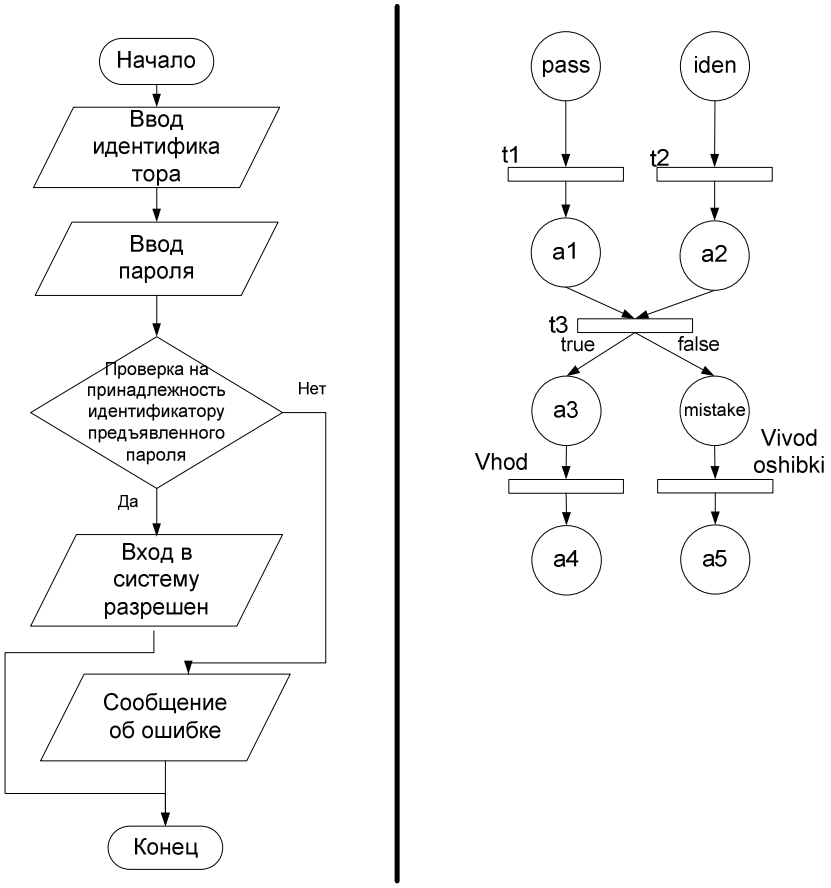

Рис. 1. Блок-схема алгоритма и сеть Петри вход пользователя в ИСПДн №1

a4 – пользователь санкционировано вошел в ИСПДн №1;

a5 – пользователь не получил право доступа в ИСПДн №1;

t1 – ввод пароля и идентификатора пользователем;

t2 – ввод идентификатора пользователем;

t3 – аутентификация пользователя в системе;

mistake – предъявленный идентификатор не соответствует введенному паролю;

vivod oshibki – вывод ошибки на экран;

vhod – идентификатор и пароль приняты.

Согласно [2] СЗКИ для ИСПДн №1 должна удовлетворять требованиям, указанным в табл. 1.

Таблица 1

Требования к ИСПДн № 1

№ п/п	Наименование подсистемы	Требования
1.	Управление доступом	♦ идентификация и проверка подлинности пользователя при входе в систему ИС по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
2.	Регистрация и учет	♦ регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова; ♦ учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета;
3.	Обеспечение целостности	♦ обеспечение целостности программных средств СЗКИ, обрабатываемой информации, а также неизменность программной среды; ♦ периодическое тестирование функций СЗКИ при изменении программной среды и пользователей ИС с помощью тест-программ, имитирующих попытки несанкционированного доступа; ♦ наличие средств восстановления СЗКИ, предусматривающих ведение двух копий программных компонентов СЗКИ, их периодическое обновление и контроль работоспособности

На рис. 2 показана блок-схема алгоритма и сеть Петри для реализации требования к СЗКИ по управлению доступом и использованы следующие обозначения:

pass – пароль, введенный пользователем для аутентификации (фишка типа 1 – правильный пароль, который соответствует всем требованиям; фишки другого типа – неправильные и (или) некорректные пароли);

iden – идентификатор, который использует пользователь для идентификации в системе (фишка типа 2 – идентификатор корректен и удовлетворяет всем условиям; фишки другого типа – неправильные и (или) некорректные идентификаторы);

A1 – пароль введен пользователем в окно запроса пароля;

A2 – пароль, введенный пользователем, единственный в БД паролей;

A3 – пароль содержит не менее шести символов, среди которых имеются буквы и цифры;

A4 – идентификатор введен пользователем;

A5 – предъявленный идентификатор подтвержден введенным паролем, аутентификация прошла успешно;

T1 – ввод пароля в окно запроса пароля;

T2 – проверка единственности пароля в БД паролей;

T3 – проверка введенного пароля согласно установленным ограничениям по длине (не менее шести символов), а также на наличие в нем букв и цифр;

T4 – аутентификация пользователя в системе;

T5 – ввод идентификатора пользователем;

mistake – предъявленный идентификатор не соответствует введенному паролю;

vivod oshibki – вывод ошибки на экран;

vhod – идентификатор и пароль приняты.

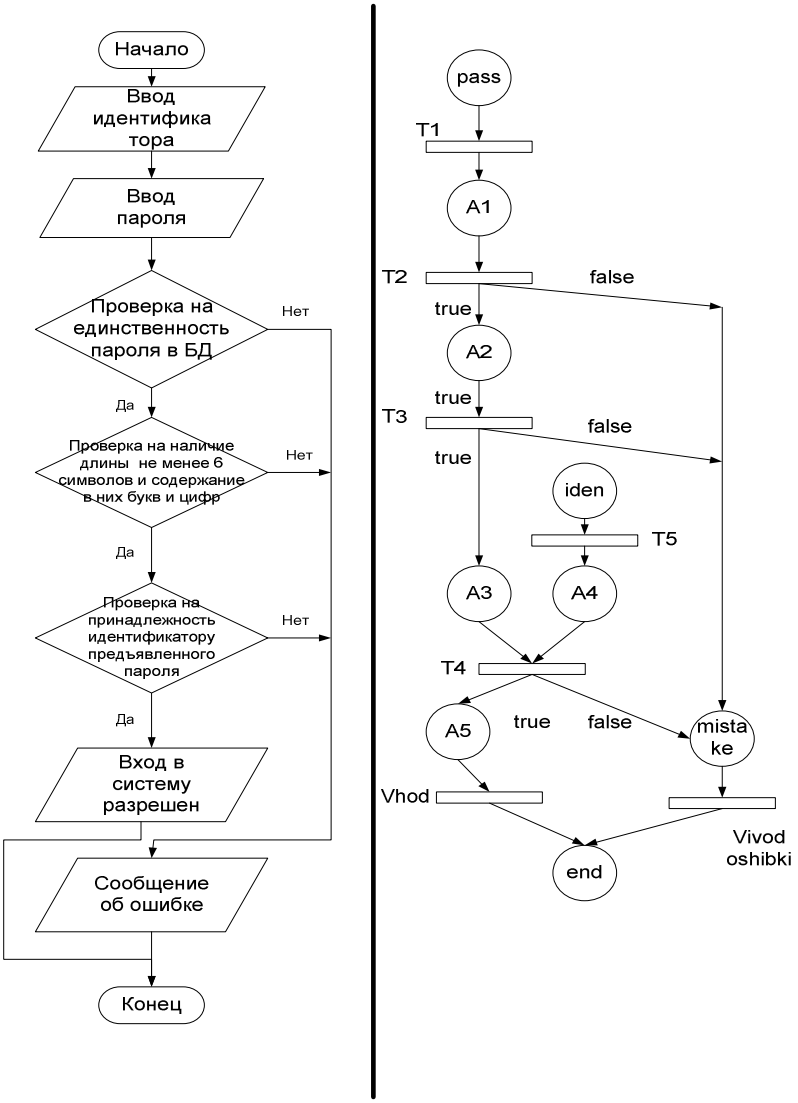

Рис. 2. Блок-схема критерия и сеть Петри

Цвет фишек сети Петри, построенной для реализованной в ИСПДн №1 подсистемы управления доступом красный, а для подсистемы управления доступом согласно требованиям нормативно-законодательной базы – зеленый.

На рис. 3 фишками красного цвета отмечены требования, реализованные в ИСПДн №1, а зеленого цвета – требования согласно [2].

На рис. 3 показано, что подсистема управления доступом, которая используется в ИСПДн №1, имеет ряд недостатков относительно требований законодательной базы РФ. А именно, в подсистеме управления доступом не реализовано требование по проверке пароля на содержание в нем не менее шести символов, среди которых имеются буквы и цифры. Поэтому используемые механизмы защиты в подсистеме управления доступом в ИСПДн №1 являются противоречивыми и недостаточными. Проектируя СЗКИ необходимо учесть недостатки ранее реализованной подсистемы управления доступом и устранить их.

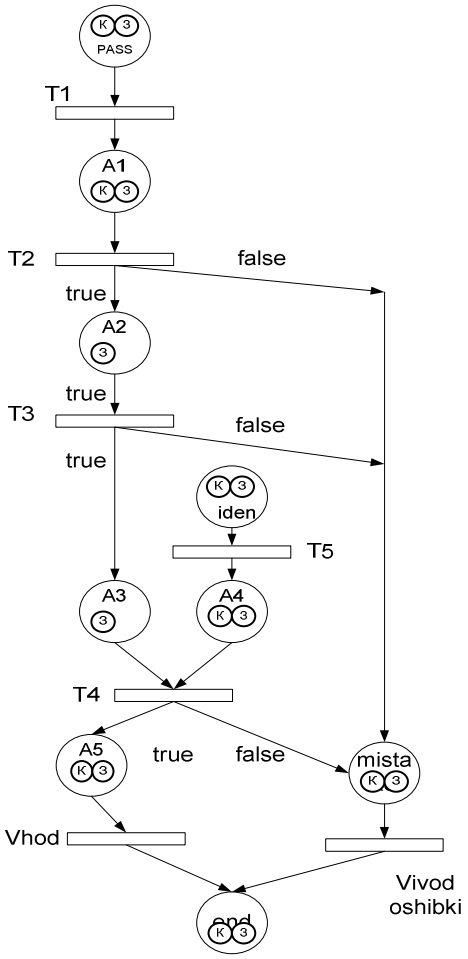

Рис. 3. Раскрашенная сеть Петри для подсистемы управления доступом

Выводы:

1. Согласно [5] существует несколько видов конфиденциальной информации. В статье приведен пример анализа подсистемы управления доступом для системы обработки ПДн, который показал недостаточность применяемых мер защиты.
2. Аппарат сети Петри является средством моделирования различных ИС и СЗКИ, и дает возможность получить информацию о структуре и динамическом поведении ИС, СЗКИ и тем самым спроектировать надежную СЗКИ, а использование фишек различных цветов при проведении обследования СЗКИ позволяет выявить уязвимые места ИС и СЗКИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шелупанов А.А., Миронова В.Г. и др.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 1 (21). – Ч. 1. – С. 14-22.
2. «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» // Приказ Федеральной службы по техническому и экспертному контролю Российской Федерации от 5 февраля 2010 г. № 58.
3. *Котов В.Е.* Сети Петри. – М: Наука, 1984.

4. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
5. Указ Президента Российской Федерации от 23.09.2005 г. №1111 «Перечень сведений конфиденциального характера».
6. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 2 (22). – Ч. 1. – С. 257-259.

Статью рекомендовал к опубликованию к.ф.-м.н. Г.А. Афонин.

Миронова Валентина Григорьевна
Томский государственный университет систем управления и радиоэлектроники.
E-mail: mvg@security.tomsk.ru.
634050, г. Томск, пр. Ленина, 40.
Тел.: 89234151608.
Кафедра комплексного обеспечения информационной безопасности электронно-вычислительных систем; аспирант.

Шелупанов Александр Александрович
E-mail: saa@udcs.ru.
Проректор по научной работе; д.т.н.; профессор.

Mironova Valentina Grigor'evna
Tomsk State University of Control Systems and Radioelectronics.
E-mail: mvg@security.tomsk.ru.
40, Lenin Pr., Tomsk, 634050, Russia.
Phone: +79234151608.
The Departmant of Integrated Information Security Computer Systems; Postgraduate Student.

Shelupanov Alexander Alexandrovich
E-mail: saa@udcs.ru.
Vice Rector for Research; Dr. of Eng. Sc.; Professor.

УДК 004.05

О.М. Лепешкин, Р.С. Гаппоев

МАНДАТНАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

Исследование в области защиты информации и вычислительной техники показывает, что в развитых странах мира уже давно сложилась инфраструктура безопасности информации в системах обработки данных, которая нуждается в рассмотрении для систем реального времени. Внедрение системных требований международных стандартов и принципов процессного подхода в системы управления, приводит к изменению принципов контроля безопасности и требует пересмотра основных подходов по построению систем безопасности в динамике.

Вследствие этого, в данной статье проведен анализ основных моделей разграничения доступа на основе мандатной политики безопасности: «Белла – Лападула» и «Китайской стены», для систем реального времени. Выявлены основные недостатки и противоречия (деклассификация объектов) этих моделей, которые потенциально могут нарушать безопасность системы. Для устранения этих проблем предлагается рассмотреть модель предоставления прав доступа на основе «полномочий субъекта» и «допуска полномочий у объекта». Для реализации данного метода было решено использовать среду радикалов, основой которых являются предикаты.

Политика безопасности; мандатные модели; мандатный доступ; контроль целостности; схемы радикалов.