подается последовательность транзакций, выходом модели служит класс, определяющий, является ли данная последовательность транзакций потенциально опасной или нет. С помощью решения этой задачи, возможно сделать вывод о безопасности авторизации текущей транзакции.

Данные для решения задачи прогнозирования отличаются лишь меткой: бинарный вариант {0,1} неприменим, необходимо ввести непрерывную величину. Введем параметр $A = N_0*Q_0 - N_1*Q_1$, где N_1 — вес мошеннической транзакции, N_0 — вес законной транзакции ($N_1 > N_0$). На вход модели прогнозирования поступает последовательность транзакций (текущая + ретроспективные), на выходе — прогнозируемое число A, которое условно можно назвать риском транзакции, и далее эксперт (или другой алгоритм) может оценить, насколько разумной является авторизация данной транзакции. Этим алгоритмом может быть классификатор, на входе которого будет уже не последовательность транзакций, а число A. Такую задачу классификации решить проще, так как входное множество — не массив сложно структурированных данных, а конкретное число. Таким образом, последовательное решение задач прогнозирования и классификации также может быть применено для выявления несанкционированных операций.

Разработанный подход может в дальнейшем стать основой для модуля выявления мошеннических транзакций с использованием методов ИАД.

СПИСОК ЛИТЕРАТУРЫ:

1. Курс лекций Data Mining. Интернет-университет информационных технологий. URL: http://www.intuit.ru/department/database/datamining/.

А. А. Балаев, В. С. Горбатов

МЕТОДИКА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ PLC-СЕТЕЙ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В связи с принятием Федерального закона № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации» становится актуальной задача повышения эффективности управления системами информационной безопасности территориально-распределенных систем энергообеспечения. Для решения указанной задачи в системах электропитания представляется целесообразным применение распределенных систем передачи данных на основе технологии powerline communication (PLC) [1]. Однако в настоящее время никаких общих решений по вопросам обеспечения информационной безопасности таких сетей еще не предложено, что затрудняет оценку их защищенности.

В данной работе предлагается методика проведения проверки PLC-сети на соответствие требованиям безопасности информации, которая основывается на положениях руководящих документов ФСТЭК России [2] и типовых методиках испытаний объектов информатизации по требованиям безопасности информации и включает в себя:

1. Структурную модель PLC-сети;
2. Модель угроз и модель нарушителя;
3. Программно-аппаратную имитацию PLC-сети;

4. Описание различных атак на PLC-сеть;

5. Рекомендации по обеспечению защиты информации в PLC-сети.

Структурная модель (рис. 1) представляет собой распределенную PLC-сеть, состоящую из пяти различных блоков [3]. Причем отдельные блоки функционирования не являются организациями.

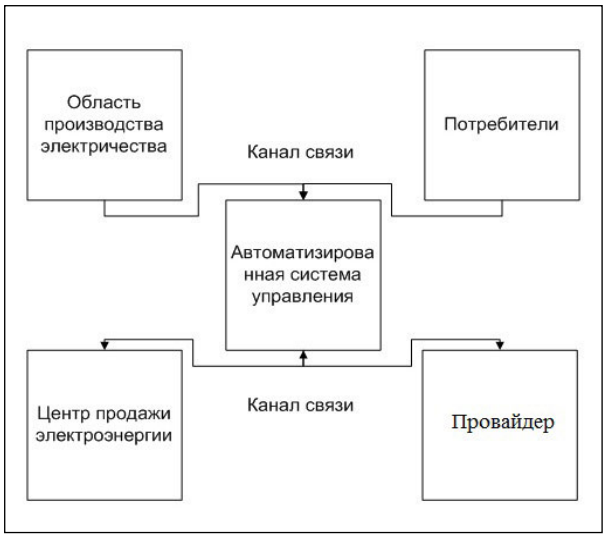

Рис. 1. Структурная модель распределенной PLC-сети

На основе модели (рис. 1), построены модель нарушителя, модель угроз и описаны результаты успешной реализации угроз. По результатам проделанной работы, разработана методика аттестационных испытаний распределенной PLC-сети по требованиям безопасности информации.

СПИСОК ЛИТЕРАТУРЫ:

1. HomePlug Powerline Alliance. URL: https://www.homeplug.org/home.
2. ФСТЭК России. URL: http://fstec.ru.
3. IEEE & SMART GRID. URL: http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model.

А. А. Балаев, Н. Н. Пантелеева, А. Э. Нигулас

СОЗДАНИЕ МОБИЛЬНОЙ ЭКРАНИРОВАННОЙ ПАЛАТКИ

Целью проекта является создание мобильной экранированной палатки для снижения индустриальных радиопомех (ИРП) при проведении специальных исследований для выявления с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем [1].

ИРП возникают при работе электрических, электронных и радиотехнических устройств различного назначения [2]. Для проведения эффективных специсследований технических средств необходимо либо проводить радиомониторинг, т. е. создавать базу данных окружающего фона на