УДК 681.3

# СЕТИ ПЕТРИ, ИЛЛЮСТРИРУЮЩИЕ МОШЕННИЧЕСКУЮ ОПЕРАЦИЮ С БАНКОМАТОМ ПОСРЕДСТВОМ ВНЕДРЕНИЯ ВИРУСА, КАК РАЗНОВИДНОСТЬ ДЕЯТЕЛЬНОСТИ ИНСАЙДЕРОВ

**Р.В. Менжулин, Д.М. Коваленко**

Приведена модель взаимодействия нарушитель – банкомат, результатом взаимодействия которого является мошенническая операция с банкоматом посредством внедрения вируса

Ключевые слова: вирус, банкомат, инсайдер

Компьютерные вирусы представляют серьезную угрозу для информационной безопасности платежных систем на банковских картах с магнитной полосой. Объектами заражения являются сети банкоматов. Попадая в банкомат, вирус копирует данные о проведенных транзакциях (номер счета, ПИН – код, ФИО держателя карты, кодированные данные магнитной полосы, перемещение денежных средств по данному банковскому счету) и записывает их в текстовый файл, в порядке проведения клиентами операций. Данные операции повторяются на некотором интервале времени (n+1), до того момента времени (n+2), когда нарушитель, путем набора на клавиатуре определенной комбинации цифр, получает доступ к файлу с данными о проведенных транзакциях. Далее злоумышленник выводит эти данные на слипе (чек). По полученным данным изготавливаются поддельные банковские карты, в то время как держатели оригинальных карт ничего об этом не подозревают.

Вирус не может проникнуть в банкомат через внешнюю сеть, потому что все транзакции осуществляются в режиме Off – line. Злоумышленник также не сможет загрузить вирус из внешней среды, так как это возможно только при техническом взаимодействии (человек – банкомат), а банкоматы обладают достаточной степенью защиты как внешне, так и внутренне[2]. Следовательно, вирус может быть загружен человеком, имеющим непосредственный доступ к банкомату, то есть сотрудником банка или процессингового центра, обеспечивающего техническое функционирование сети банкоматов. Таких людей называют инсайдерами. Инсайдер – это человек, работающий в компании, который может распространять конфиденциальную информацию, в определенных целях[1]. В данном случае конфиденциальной информацией является информация, нанесенная на банковскую карту. Из вышесказанного следует, что в данном случае инсайдер является злоумышленником.

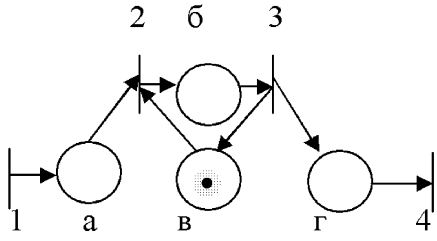
Процессы взаимодействия злоумышленника с банкоматом в различные интервалы времени показаны на рисунке на основе сетей Петри. На рисунке (а) изображен интервал времени, в котором злоумышленник загружает вирус в банкомат. События: 1 – Прибытие злоумышленника; 2 – Процесс загрузки вируса активирован; 3 – Процесс загрузки вируса деактивирован; 4 – Банкомат находится под воздействием вируса. Условия: а – Злоумышленник прибыл и готов к загрузки вируса; б – Банкомат находится под воздействием злоумышленника; в - Банкомат не занят; г – Процесс загрузки вируса прошел успешно.

На рисунке (б) показан процесс взаимодействия банкомата с клиентом. События: 1 – Ожидание прибытия клиента; 2 – Клиент начинает транзакцию; 3 – Завершение транзакции; 4 – Транзакция проведена. Условие: а – Клиент прибыл и готов к началу операции; б – Банкомат выполняет транзакцию, находясь под воздействием клиента и вируса; в – Банкомат не занят; г – Клиент не занят; д – Успешное

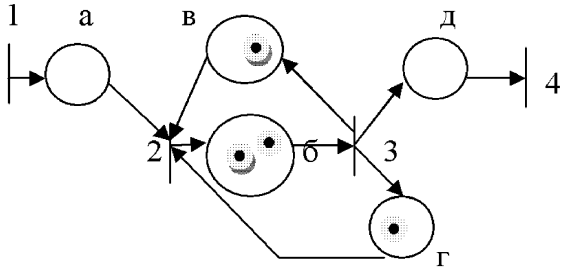
Менжулин Роман Валерьевич - ООО Инженерно – производственно – коммерческая фирма “Универсал - Интер”, ведущий специалист по информационной безопасности, e-mail: Roman009.86@mail.ru

Коваленко Дмитрий Мифодиевич – Воронежский ИВЦ структурное подразделение ГВЦ филиала ОАО РЖД, специалист по защите информации, тел. 89204041521

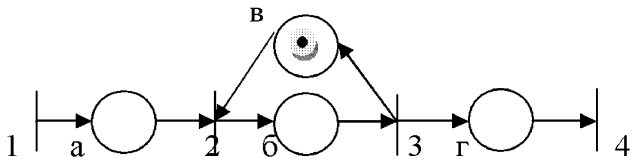
проведение транзакции. На рисунке (в) иллюстрирован процесс взаимодействия злоумышленника с банкоматом в момент времени (n+2). События: 1 – Прибытие злоумышленника; 2 – Злоумышленник начинает операцию по выводу скопированных данных; 3 – Завершение операции; 4 – Злоумышленник владеет необходимой информацией. Условия: а – Злоумышленник прибыл и готов к началу операции; б – Банкомат под воздействием злоумышленника; в – Банкомат не занят; г – Операция произведена успешно.




а) n – й интервал времени




б) (n + 1) – й интервал времени




в) (n + 2) – й интервал времени

Сети Петри, иллюстрирующие взаимодействие инсайдера с банкоматом

Анализ данных сетей позволяет сделать вывод, что нерегулярное проведение оценки рисков, а также недостаток либо полное отсутствие инвестиций в работе по снижению рисков, связанных с человеческим фактором (некорректное поведение сотрудников, оплошность, нарушение установленных правил или стандартов), образуют серьезную угрозу для платежных систем на банковских картах. Основное внимание по-прежнему уделяется лишь таким внешним угрозам, как вирусы, а серьезность внутренних угроз недооценивается.

Литература

1. Банковская система России. Настольная книга банкира.. - М.: Декабрь, 2005. Кн. III. с. 382.

2. Калугин Н.М., Кудрявцев А.В., Савинская Н.А. Банковская коммерческая безопасность: учебн. пособие / под ред. Г.А. Краюхина. - СПб.: СПб. ГИЭА, 2000 с.

ООО ИПКФ Универсал – Интер
Воронежский ИВЦ структурное подразделение ГВЦ филиала ОАО РЖД
Universal – Inter, LTD
The Voronezh data-processing centre structural division GVTS of branch of Open Society of the Russian Railway

## NETWORKS PETRI ILLUSTRATING ROGUISH OPERATION WITH THE CASH DISPENSE, BY MEANS OF VIRUS INTRODUCTION, AS THE VERSION OF ACTIVITY INFINGERS

**R.V. Menzhulin, D.M. Kovalenko**

The model of interaction the infringer – a cash dispense which result is roguish operation with a cash dispense, by means of virus introduction is resulted

Key words: virus, cash dispense, infinger