А.В. Климов
(НИЦ "Охрана" МВД России; e-mail: avk031@mail.ru)

ИНФОРМАЦИОННЫЕ ХАРАКТЕРИСТИКИ СИГНАЛОВ, ВОЗНИКАЮЩИХ ПРИ ВЗЛОМАХ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ

Представлены результаты экспериментальных исследований процессов и сигналов, возникающих при разрушающих воздействиях на банкоматы с использованием различных инструментов. Смоделированы типичные криминальные способы взлома. Приведены примеры амплитудно-временных и спектральных характеристик сигналов.

Ключевые слова: банкоматы, взлом, процессы, сигналы.

A.V. Klimov

INFORMATION CHARACTERISTICS OF THE SIGNALS, OCCURS WHEN HACKING AUTOMATED TELLER MACHINE

Presents the results of experimental researches of processes and signals arising from the application of the damaging effects on automated teller machines using different tools. Simulated typical criminal ways of hacking. Examples of amplitude-temporal and spectral characteristics of the signals are given.

Key words: automated teller machine, hacking, processes, signals.

Статья поступила 10 декабря 2014 г.

В последние годы в России наблюдается активное развитие системы дистанционного банковского обслуживания и национальной платежной системы и, как следствие, значительное увеличение числа банкоматов и платежных терминалов. Их общее количество уже превышает 200 тысяч.

Вместе с тем, растет и количество криминальных посягательств на банковские устройства самообслуживания с целью кражи размещенных в них наличных денежных средств. По статистике МВД России, в 2013 году было зафиксировано 1357 уголовных преступлений, связанных со взломом банкоматов и платежных терминалов и хищением из них наличных денежных средств. Это на 9 % больше, чем в предыдущем году [1]. Примерно в 60 % случаев банковские устройства самообслуживания взламывают на месте установки, в остальных случаях – банкоматы или платежные терминалы похищают целиком и взламывают в удаленном скрытом месте.

Применение традиционных средств обнаружения оказывается неэффективным. Приставить физическую охрану к каждому банкомату или поставить все банкоматы под постоянный и качественный видеоконтроль (в режиме "on-line") практически невозможно.

Поэтому для защиты банковских терминалов необходимо создание современных и высокоэффективных автоматических средств обнаружения, которые могли бы на максимально раннем этапе определить попытку взлома или кражи банковского устройства самообслуживания и сообщить об этом в службу охраны (безопасности) для оперативного реагирования по пресечению преступления.

С целью определения возможности создания таких технических средств, в НИЦ "Охрана" МВД России были проведены экспериментальные исследования процессов и сигналов, возникающих при взломе банкоматов и платежных терминалов, в том числе сейфов, в которых хранятся кассеты с наличными денежными средствами.

Исследования проводились с сейфами, банкоматами (рис. 1) и платёжными терминалами (рис. 2), предоставленными ведущими российскими производителями и поставщиками банковского оборудования – ЗАО "Новый город" и Московским банком ОАО "Сбербанк России".

Рис. 1. Банкоматы, предоставленные для экспериментальных исследований

Рис. 2. Платежные терминалы, предоставленные для экспериментальных исследований

Экспериментальные исследования проводились путём воспроизведения физических процессов взлома верхнего кабинета банкомата (рис. 3), где расположены аппаратно-программные модули управления, связи и пользовательского интерфейса, а также нижнего кабинета банкомата (рис. 4), где расположен сейф с кассетами, в которых находятся наличные денежные средства. Одновременно с этим осуществлялись измерения, записи, амплитудно-временной и спектральный анализы виброакустических сигналов, возникающих при нанесении разрушающих воздействий, а также сигналов, возникающих при штатной работе механизмов банкоматов и платежных терминалов, при осуществлении банковских операций, загрузке, выгрузке и техническом обслуживании.

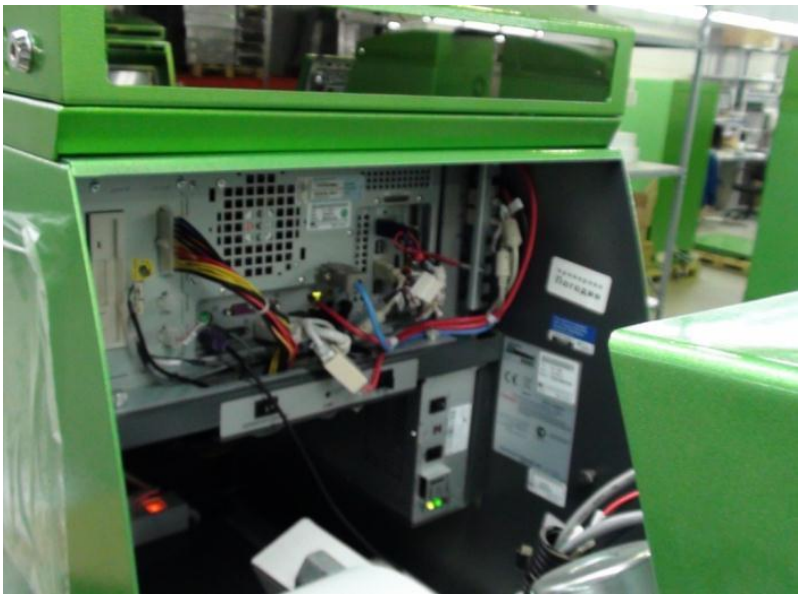

Рис. 3. Внешний вид программно-аппаратных модулей, расположенных в верхнем кабинете банкомата

Рис. 4. Внешний вид кассет с наличными деньгами в нижнем кабинете банкомата

Исследования проводились в испытательной лаборатории НИЦ "Охрана" МВД России (г. Москва) и на производственно-испытательной базе ЗАО "Новый Город" (г. Фрязино Московской области) с использованием регламентированных по ГОСТ Р 50862-2012 [2] средств и методов криминального вскрытия (взлома) банковских средств защиты (табл. 1).

Таблица 1

Категории, технические характеристики и виды инструментов

Категории инструментов по ГОСТ Р 50862-2012	Виды инструментов	Технические характеристики инструментов
А	Электродрель	Электрический неударный, мощность до 500 *Вт*, масса до 3 *кг*
А	Пила, напильник	Ручной режущий, масса до 1,5 *кг*, длина до 400 *мм*
А	Молотки, кувалды, колуны, кирки	Ручной ударный, масса головки до 1,5 *кг*, длина рукояти до 750 *мм*
В	Газорежущее, сварочное оборудование	Термический режущий с расходом кислорода до 50 $дм^3/мин$
В	Электрические дисковые пилы	Электрические режущие и шлифовальные инструменты мощностью до 800 *Вт* с абразивным диском

Процесс разрушения двери сейфового отсека банкомата электродрелью показан на рис. 5.

Рис. 5. Процесс разрушения электродрелью

В результате эксперимента пороговый уровень сигнала составил 1,5-2 % от калибровочного уровня (U_0). При этом, согласно спектральной характеристике сигнала, наиболее эффективная часть спектра находится в диапазоне частот от 4,8 до 9,5 *кГц*.

Процесс разрушения сейфового отсека банкомата электрической дисковой пилой показан на рис. 6.

Рис. 6. Процесс разрушения сейфового отсека банкомата электрической дисковой пилой

Как показал анализ временной характеристики сигнала, пороговый уровень сигнала составил 5-7 % от калибровочного уровня (U_0). При этом наиболее эффективная часть спектра находится в диапазоне частот от 6,2 до 9,5 *кГц*.

Процесс разрушения сейфового отсека банкомата газовым (кислородно-ацетиленовым) резаком показан на рис. 7.

Рис. 7. Процесс разрушения сейфового отсека банкомата газовым резаком

В результате эксперимента пороговый уровень сигнала составил 2-3 % от калибровочного уровня (U_0). Наиболее эффективная часть спектра находится в диапазоне частот от 3,5 до 11,0 *кГц*.

В процессе разрушения банкомата с использованием газового резака было произведено измерение температуры воздуха внутри сейфового отсека банкомата. При этом времени от начала воздействия до момента сквозного прожигания корпуса сейфового отсека банкомата составило примерно 25 *с*. В течение этого времени температура воздуха, первоначально зафиксированная на уровне 21 °*C*, оставалась практически неизменной.

После прожигания сквозного отверстия наблюдался быстрый рост температуры воздуха внутри банкомата со скоростью $V(t)$, °*C*/*мин*, определяемой [4-6] по формуле:

$$V(t) = 60\frac{T_2 - T_1}{t_2 - t_1}, \quad (1)$$

где T_1 – температура воздуха в сейфовом отсеке банкомата в начале термического воздействия на банкомат, °*C*;

T_2 – температура воздуха в сейфовом отсеке банкомата в конце термического воздействия на банкомат, °*C*;

t_1 – момент времени начала прожигания сквозного отверстия в корпусе сейфового отсека банкомата, *с*;

t_2 – момент времени завершения термического воздействия на банкомат, *с*.

По формуле (1), средняя скорость нарастания температуры воздуха в сейфовом отсеке банкомата при сквозном термическом разрушении его корпуса составляет:

$$V(t) = 60\frac{60 - 21}{46 - 27} = 123 \ ^\circ C/мин. \quad (2)$$

Следующий вид воздействия – нанесение ударов по петле двери сейфового отсека банкомата молотком и зубилом.

В данном эксперименте пороговый уровень сигнала достиг 100 % калибровочного уровня (U_0). Вместе с тем, каждый такой сигнал имел относительно небольшую длительность (примерно 10 *мс*). При этом максимальные значения контролируемых уровней сигнала находились в диапазонах частот от 150 до 200 *Гц*, в районе 300 *Гц* и в диапазоне частот от 500 *Гц* до 2,5 *кГц*.

По результатам проведенных экспериментальных исследований процессов и сигналов, возникающих при взломе банковских устройств самообслуживания (банкоматов и платежных терминалов), можно сделать следующие выводы:

1. Анализ полученных данных позволяет утверждать, что информационные характеристики виброакустических сигналов, возникающих при взломе различными инструментами, имеют особенности, которые можно использовать для их селекции на фоне характерных шумов и помех, возникающих в процессе эксплуатации банковских средств защиты и устройств самообслуживания.

2. Полученные высокие значения амплитуды и скорости нарастания температуры воздуха в сейфовом отсеке банкомата при сквозном термическом разрушении его корпуса дают основания полагать, что данные параметры могут быть использованы как дополнительные информационные признаки взлома банкомата, осуществляемого с использованием газорежущего оборудования.

3. При использовании дополнительных методов обработки полученные информационные характеристики сигналов могут быть использованы при создании автоматического модуля охранной сигнализации.

Литература

1. ***Климов А.В.*** Специализированный модуль для комплексной охраны средств хранения финансов и дистанционного банковского облуживания // Матер. 23-й междунар. науч.-техн. конференции "Системы безопасности – 2014". М.: Академия ГПС МЧС России. 2014. С. 337-339. http://ipb.mos.ru/sb.

2. ***ГОСТ*** Р 50862-2012. Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость.

3. ***ГОСТ*** Р 53325-2012. Техника пожарная. Технические средства пожарной автоматики. Общие технические требования и методы испытаний.

4. ***Членов А.Н., Буцынская Т.А.*** Акустические методы обнаружения пожара // Технологии техносферной безопасности. 2008. Вып. № 2. http://ipb.mos.ru/ttb.

5. ***Членов А.Н.*** Раннее обнаружение пожара системами противопожарной защиты объектов // Матер. 22-й междунар. науч.-техн. конф. "Системы безопасности – 2013". М.: Академия ГПС МЧС России. 2013. С. 262-265. http://ipb.mos.ru/sb.

6. ***Членов А.Н., Буцынская Т.А., Шакирова А.Ф., Федоров В.Ю.*** Групповой извещатель для тревожной сигнализации // Пожары и чрезвычайные ситуации: предотвращение, ликвидация. № 1. М.: Академия ГПС МЧС России, 2011. С. 42-46.