Протоколирование, оповещение и блокировки. ДД выполняет записи в протокол безопасности как самостоятельно, так и по команде от клиентских приложений. Самостоятельно протоколируются плановые действия такие, как вход пользователя в систему, изменение прав доступа к объектам, выдача объектов пользователям для просмотра и редактирования.

Также ДД протоколирует события, которые могут рассматриваться как попытки несанкционированного доступа, например, запрос объекта, не стоящего на контроле ДД. По команде с клиентских приложений протоколируются так называемые «события второй категории», например, отрицательный результат проверки электронной подписи пользователя под конкретным файлом, что может быть следствием искажения содержащегося в файле документа при его хранении или передаче по каналам связи.

Для событий, требующих немедленного вмешательства администратора безопасности, должна быть предусмотрена отправка ДД сообщения на АРМ аудитора системы (он же АРМ администратора безопасности ОС).

Должна быть предусмотрена также возможность блокировки документов в случаях, когда администратору безопасности необходимо прекратить работу пользователей системы с документом для расследования внештатных ситуаций (попытки несанкционированного доступа, некорректные действия сотрудников).

В этом случае документ блокируется по команде с АРМ администратора ОС или с клиентского рабочего места (автоматически, скрытно от пользователя), после чего этот документ не может быть выдан ни одному пользователю, кроме администратора безопасности. Разблокирование документа доступно только администраторам безопасности.

Алгоритм работы диспетчера доступа. Алгоритм функционирования диспетчера доступа к документам для операционной системы Astra Linux состоит в следующем:

– пользователь обращается к web-серверу с запросом на доступ;

– сервер проверяет результаты идентификации пользователя (в случае использования сервиса Astra Linux Directory и единого пространства пользователей) или запрашивает у пользователя логин и пароль для собственной автономной процедуры идентификации и аутентификации;

– в случае если пользователь успешно идентифицирован, web-сервер предоставляет пользователю список документов, иначе передается сообщение об отказе в доступе;

– пользователь выбирает документ из предоставленного списка документов;

– web-сервер передает запрос на доступ (в составе идентификатора документа, идентификатора пользователя, типа доступа) программному модулю диспетчера доступа;

– модуль диспетчера доступа проверяет установленные права доступа к документу для пользователя, по идентификатору документа из запроса и идентификатору пользователя из запроса;

– при разрешении на доступ модуль диспетчера доступа возвращает web-серверу карточку документа (список файлов и метаданные документа);

– при отказе в доступе модуль диспетчера доступа возвращает web-серверу сообщение об отказе в доступе.

Литература

1. П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко, В.Г Проскурин, А.Н. Цибуля: Безопасность операционной системы специального назначения Astra Linux Special Edition, М. Учебное пособие для вузов / Под редакцией доктора тех. наук П.Н. Девянина.

2. А.А. Грушо, Э.А. Применко, Е.Е. Тимонина: Теоретические основы компьютерной безопасности, учебное пособие для студентов высших учебных заведений / Издат.центр «Академия», 2009.

УДК 519.712.2

ЭКСПЕРИМЕНТАЛЬНЫЕ ОЦЕНКИ МИНИМАЛЬНОЙ ДЛИНЫ РАЗДЕЛЯЮЩЕЙ ПОСЛЕДОВАТЕЛЬНОСТИ ЛЕЖАНДРА

Лебедев А.Н., Кокорин А.О., Савельев Е.Д.

Московский государственный технический университет имени Н. Э. Баумана
Москва, Российская Федерация

Введение. Для создания специализированных микроконтроллеров, реализующих оптимальным образом однонаправленные функции криптографических преобразований, составляющих базовые компоненты протокола выработки общего секрета Диффи – Хеллмана важно точно представлять на какой минимальной длине различных двоичных представлений чисел по модулю большого простого числа можно гарантировать однозначность такого представления чисел. Поэтому мы провели целый ряд экспериментальных исследований, позволяющих выдвинуть достаточно обоснованные гипотезы о характере поведения минимальной длины такого представления на основе последовательностей Лежандра.

Дадим определение последовательности Лежандра [1]. Пусть p – простое число. Целое число a называется квадратичным вычетом по модулю p,

если разрешимо сравнение $x^2 \equiv a \pmod p$. Если указанное сравнение не разрешимо, то число a называется квадратичным невычетом по модулю p.

Символ Лежандра – это функция от двух аргументов a и p, которая определяется как:

(a|p) = 1, если число a является квадратичным вычетом по модулю p;

(a|p) = -1, если число a не является квадратичным вычетом по модулю p (в этом случае говорят, что a является квадратичным невычетом по модулю p).

Последовательность Лежандра длины n с началом в точке a – это последовательность значений символа Лежандра на последовательных значениях аргумента a: т. е. это последовательность значений символа Лежандра вида ((a+i)|p), где i = 0, 1, 2, …, n-1.

По малой теореме Ферма для любого простого числа p последовательность Лежандра достаточно большой длины, начинающаяся с любого уелого числа a является периодической с периодом p – 1.

Рассмотрим значения минимальной длины последовательности Лежандра для заданного простого числа p, при которой все подпоследовательности Лежандра, имеющие длину не менее данной величины уникальны в бесконечной периодической последовательности Лежандра, построенной для заданного простого числа p. Для этого мы реализовали компьютерную программу расчета минимальной длины, при которой различаются все подпоследовательности Лежандра, имеющие длину не менее заданной величины. Алгоритм расчета этой минимальной длины разделяющей подпоследовательности Лежандра выглядит следующим образом. Алгоритм:

1. Возьмем простое число p.

2. Построим мультипликативную конечную циклическую группу по модулю данного простого числа p. Группа эта будет состоять из p-1 элемента, а именно – из степеней любого первообразного по модулю p элемента a – образующего эту циклическую группу $\{a, a^2, a^3, a^4, \ldots, a^{n-1} = 1\}$

3. Возьмем циклическую последовательность целых чисел: 1, 2, 3…, p-1, 1, 2,…, p-1, 1, 2, … Каждому элементу этой последовательности поставим в соответствие значение 1 или -1 в зависимости от четности степени данного числа в данной конечной циклической группе.

4. Получим последовательность из чисел 1 и -1.

Найдем минимальную длину, при которой в построенной последовательности не будет повторяющихся подпоследовательностей.

Рассмотрим простой пример: простое число p = 23. Образующий элемент мультипликативной группы – a = 5. Мультипликативная группа, записанная по возрастанию показателя степени образующего элемента a состоит из следующих чисел {5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1}.

В таблице 1 мы сопоставляем квадратичному вычету знак "+", а квадратичному невычету – знак "-".

Таблица 1 – Последовательность Лежандра для мультипликативной группы вычетов по модулю p = 23

1	2	3	4	5	6	7	8	9	10	11
+	+	+	+	-	+	-	+	+	-	-
12	13	14	15	16	17	18	19	20	21	22
+	+	-	-	+	-	+	-	-	-	-

Результаты эксперимента. В результате работы написанной авторами компьютерной программы были получены точные значения минимальных значений длины последовательности Лежандра, начиная с которых все последовательности данной длины уникальны для простых чисел в интервале от 3 до 2450000 (см. рис. 1):

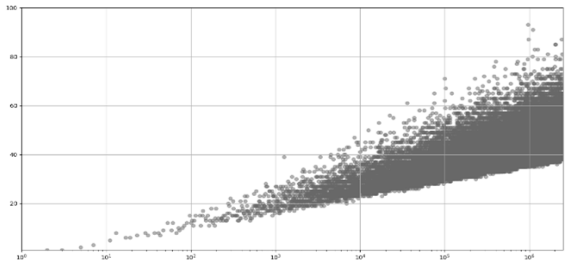

Рисунок 1 – Распределение минимальных значений длин для уникальной последовательности

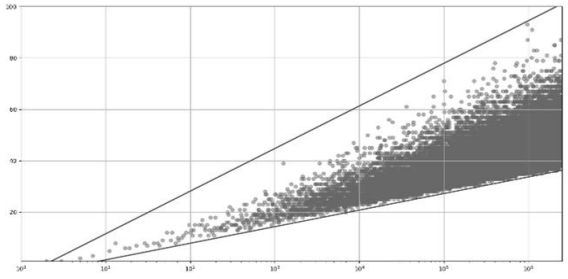

Рисунок 2 – Нижняя и верхняя границы распределения

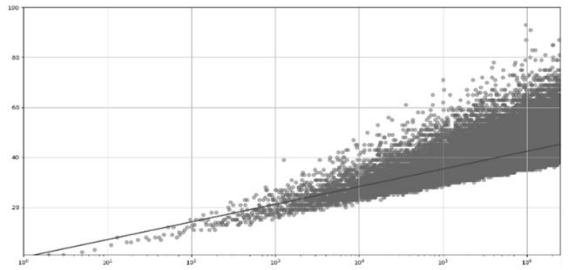

Рисунок 3 – Аппроксимация кривой 3.07ln(x)

На основе показанного на рис. 1 графика была высказана гипотеза о том, что нижняя граница распределения минимальног значения длины разделяющей последовательности Лежандра подчиняется логарифмическому закону (рис. 2).

Приблизительное значение нижней границы может быть задано следующей формулой:

$$7{,}2\ln(x) - 5.$$

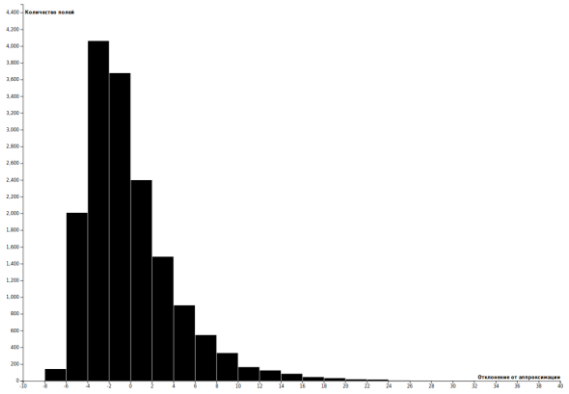

Рисунок 4 – Аппроксимация кривой 3.07ln(x)

Предположим, что распределение аппроксимируется логарифмической функцией. Тогда вычислим аппроксимирующую функцию, найдя минимальное стандартное отклонение. Получим функцию 3.07ln(x). Стандартное отклонение: 4,291 (см. Рис. 3).

Вычислим отклонения групп от аппроксимации и сведём эти значения одной диаграмме (см. рис. 4).

Видим, что большая часть групп находится вблизи нулевого отклонения, что косвенно подтверждает правильность аппроксимации логарифмической функцией 3.07ln(x).

Вывод. Предложены гипотезы аппроксимации и нижней границы распределения значений минимальной длины кодирующей последовательности с использованием последовательности Лежандра.

Литература

1. Виноградов, И.М. Основы теории чисел. / И. М. Виноградов. – Москва : Издательство Юрайт, 2018. – 102 с. – (Антология мысли). – ISBN 978-5-534-06155-0. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://biblio-online.ru/bcode/411202

2. *Манин Ю. И., Панчишкин А. А.* Введение в теорию чисел. – М.: ВИНИТИ, 1990. – Т. 49. – 341 с. – (Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления».).

3. *Нестеренко Ю. В.* Теория чисел: учебник для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2008. – 272 с.

УДК 004.056

СИСТЕМА ЗАЩИТЫ АТМ ОТ BLACKBOX АТАК НА БАЗЕ БЕСПРОВОДНОЙ ТЕХНОЛОГИИ LORA

Волков М.А., Рафиков А.Г.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

В статье рассмотрена проблема уязвимости физического канала передачи данных в АТМ к атакам типа BlackBox. Приведен обзор сетевых технологий передачи данных, на основе которого произведен выбор наиболее подходящего варианта организации связи между главным компьютером и диспенсером АТМ. Рассмотрен принцип программно-аппаратной защиты от BlackBox атак. Данная статья направлена на изучение возможностей, предоставляемых протоколом LoRa в области обеспечения информационной безопасности.

Ключевые слова: *АТМ, банкомат, безопасность, LoRaWAN, уязвимость канала передачи данных, диспенсер.*

Введение. Классическим примером Банковского устройства самообслуживания (БУС), которое необходимо защищать от злоумышленников является банкомат (**ATM** - от англ. ***Automated teller machine***) Банкомат представляет особенный интерес для злоумышленников и как непосредственное хранилище денег. Несмотря на то, что деньги хранятся в защищенном сейфе, злоумышленники находят способы добраться и до них. Помимо радикальных методов преступников, например, подрыва газом или кражи банкомата, широкое распространение последнее врем получили высокотехнологичные атаки, – на уровне программного обеспечения банкомата, сетевого взаимодействия, подсистемы управления периферийным оборудованием банкомата, а также атаки с использованием аппаратуры – BlackBox атаки.

По данным Европейской ассоциации по безопасности транзакций, за первое полугодие 2017 года в Европе было совершено 114 атак типа BlackBox (BB) [1], за 2016 г. было зафиксировано 28 случаев обнаружения BlackBox, исходя из этого рост популярности данного вида атаки составил 307 %.

Исходя из исследований, проведенных компании Positive Technologies, к BlackBox атаке уязвимы 69% рассмотренных банкоматов [2].

BlackBox атаки на АТМ. Blackbox атака - это активная атака с блокировкой передачи информации [3], злоумышленнику требуется определить факт выполнения команды (передача команды от главного компьютера к диспенсеру), перехватить эту команду, чтобы она не достигла диспенсера. Злоумышленники подключают свое устройство в канал связи между главным компьютером (системным блоком) и диспенсером, тем самым полностью контролируют проходящий через него трафик [2]. Такое подключение не вызывает особых трудностей, ведь интерфейсы системного