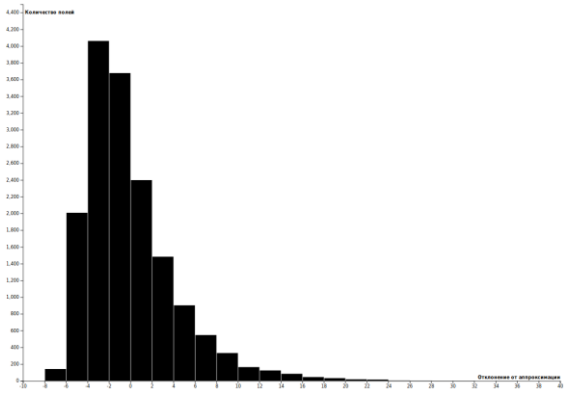

Рисунок 4 – Аппроксимация кривой 3.07ln(x)

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

блока и диспенсера стандартные, сейчас в банкоматах используются, преимущественно USB шины, предыдущие поколения АТМ использовали шины SDC (RS485) [4].

Уязвимым местом в данной атаке является канал передачи данных между главным компьютером и диспенсером [4], поскольку именно здесь происходит модификация данных. Необходимость в защите канала очевидна, необходимо добиться невозможности злоумышленником перехватывать данные канала [4], через который идут команды диспенсеру.

**Защита от BlackBox атак.** Для защиты от атак типа BlackBox создают защищенный канал передачи данных. Для этого создается устройство, которое соединяет главный компьютер с диспенсером, и шифрует весь проходящий трафик, что в теории должно обеспечить должный уровень защиты [4]. Однако, такие устройства на сегодняшний день имеют ряд недостатков. Например, наиболее распространенные устройства защиты Cerber Lock, разработка компании ANSWER Pro, и ATM Keeper, разработка компаний ООО ARTIFAKTS и ОАО КР и СО, имеют главный недостаток в том, что они устанавливаются в разрыв канала связи с диспенсером и существенно снижают надежность, и быстродействие банкомата. К тому же такие устройства на данный момент лишь частично закрывают эту проблему [4].

Альтернативой может стать создание дополнительного защищенного канала, на основе беспроводных технологий, для передачи закрытой информации: команд управления и служебной информации Подсистемы безопасности банкомата.

Дополнительно к штатному проводному соединению целесообразно добавить защищенный беспроводной канал для обмена конфиденциальной служебной информацией. При этом, дополнительный канал Подсистемы безопасности АТМ не вклинивается в штатные информационные каналы банкомата, не создает дополнительного трафика, не ухудшает параметры функционирования АТМ.

**Принцип работы предлагаемого программно-аппаратного устройства защиты от кибератак.** Особенностью *BlackBox* атак является то, что генерация команды на выдачу банкнот происходит в операционной среде банкомата или в нелегальном устройстве, напрямую подключенном к информационной шине банкомата, в то время как легальная команда поступает от процессингового сервера [4].

Предлагаемое программно-аппаратное решение (рис.1) основывается на анализе причинно-следственных связей рабочих алгоритмов, главного компьютера и оборудования банкомата, последующей передаче достоверной информации о текущих командах и ожидаемом состоянии оборудования по *безопасному беспроводному каналу связи в Систему безопасности банкомата (СББ), а именно, Блокиратору, который анализирует текущее состояние защищаемого оборудования и полученную по штатному и безопасному беспроводному каналу информацию.* Если получаемые по штатному и безопасному каналу команды, данные и данные о текущем состоянии оборудования не совпадут, то СББ зафиксирует атаку на АТМ и заблокирует его, если совпадут, то АТМ продолжит штатную работу.

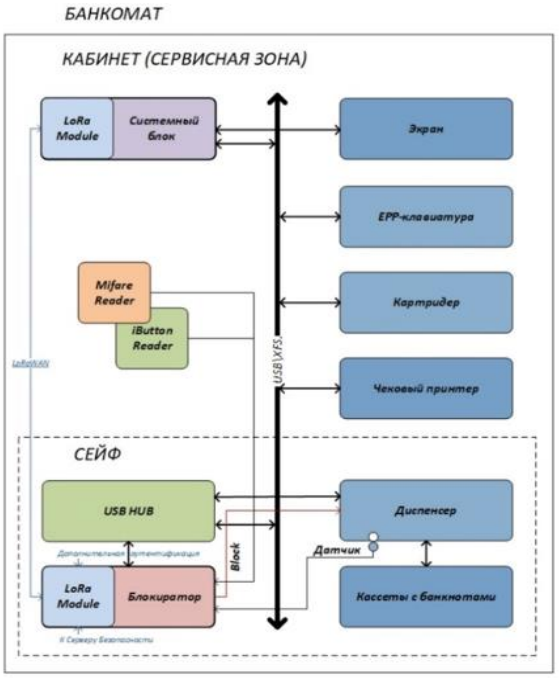


Рисунок 1 – Программно-аппаратное устройство защиты банкомата

Команда управления, сгенерированная на оборудовании злоумышленника, будет зарегистрирована системой, как несоответствующая управляющему алгоритму и модели функционирования защищаемого объекта, и будет считаться нелегальной, и не может быть проигнорирована системой безопасности, которая инициирует сигнал блокировки защищаемого объекта.

Для полноценной защиты - «Блокиратор» и комплект необходимых датчиков размещают в физически недоступном для злоумышленников отсеке – сейфе банкомата. Канал связи с системным блоком защищают от несанкционированных воздействий – для этого используют, помимо штатного канала связи – Системный блок-шина USB–USB–HUB–Dispenser, беспроводной канал обмена специализированного ПО Подсистемы безопасности банкомата (рис. 1) обеспечивают защиту информационного канала, используя криптостойкие алгоритмы защитного кодирования части управляющего трафика и взаимную

аутентификацию приемопередатчиков, подключенных к информационной шине.

В настоящее время повсеместно применяются для решения широкого круга задач различные *беспроводные протоколы передачи данных, которые эффективно могут быть использованы в Системах безопасности АТМ*.

Для обоснования выбора подходящего протокола для задач безопасности БУС рассмотрим параметры некоторых беспроводных протоколов передачи данных:

*SigFox.*

– Низкая скорость передачи данных - не более 1 кб/с;

– Малая пропускная способность сети - 140 сообщений по 12 байт в день, в случае использования сети [5, 6];

– 100 бит/с при использовании соединения M2M [5];

– Проприетарная технология;

– Не поддерживает двунаправленность обмена;

*Wheighless.*

– Синхронная сеть [6].

– Не предусмотрен режим работы M2M (конечное устройство с конечным устройством).

*GSM LTE.*

– Дорогие тарифы.

– Лицензируемые частоты.

*Стриж* (разработка компании «Стриж-телематика»).

– Использует только один канал 868 МГц.

– Проприетарная технология.

– Скорость передачи 50 б/с.

*Bluetooth.*

– Существуют проблемы с аутентификацией и приватностью [7].

– Работает на частотах 2.4 ГГц [5].

– Очень низкая проникающая способность.

Анализ существующих беспроводных протоколов показывает, что SigFox, Weightless, отечественный «Стриж», Bluetooth, включая GSM LTE, версии M2M, имеют ряд существенных недостатков, которые не позволяют использовать их для обеспечения защищенного канала обмена закрытой служебной информацией в подсистеме безопасности банкомата.

Для организации служебного защищенного канала передачи данных и команд в АТМ предлагается использовать протокол *LoRaWAN* – Long Range Wide Area Network, так как он лишен большинства недостатков своих конкурентов и обладает следующими преимуществами:

– open Sources – что позволяет самостоятельно разрабатывать ПО [8];

– имеется встроенное шифрование AES128 [8];

– имеет возможность передачи данных между конечными устройствами без использования маршрутизатора M2M [9];

– использует модуляцию в 500 кГц, что позволяет устойчиво передавать данные даже в сильно зашумленном канале;

– имеет шумоподобный сигнал, что сильно усложняет возможность выявления его из эфира;

– асинхронный – это преимущество, так как в случае синхронной передачи данных, можно отследить закономерности возникновения сигнала, тем самым скомпрометировать передачу данных [9];

– приемлемая скорость передачи данных для организации дополнительного защищенного служебного канала [6].

– используются несколько нелицензированных каналов (433 МГц и 868 МГц) – не надо платить за использование канала, можно менять канал для высокой устойчивости к помехам в эфире,

– на данный момент не выявлены случаи взлома или компрометации протокола.

– Недостатки протокола LoRa (не влияют на решение поставленных задач):

– невысокая скорость передачи данных (до 50 кб\с), зависящая от выбранного режима [8];

– чипы производят только Semtech

**Преимущество использование протокола LoRa в системе защиты АТМ от BlackBox атак.** Для построения надежной защиты АТМ от Blackbox атак необходимо использовать криптозащищенный протокол, со встроенным шифрованием [8]. Протокол LoRa наилучшим образом отвечает всем требованиям к протоколам для организации безопасного беспроводного канала связи между компонентами системы безопасности АТМ. Преимущество полнодуплексной передачи данных позволяет не тратить время на прослушивание канала [10], а несинхронность передачи позволяет избежать выявления закономерностей в канале.

Основной способ применения протокола LoRa в СББ (система безопасности банкомата) АТМ – организация служебного канала типа M2M [10].

По каналу LoRa будет передаваться только критичная информация, к примеру, сессионный ключ, или контрольная сумма, передаваемых команд по основному каналу связи USB [4]. Так как USB остается основным каналом передачи команд на диспенсер, злоумышленник захочет модифицировать команды диспенсера. Но у него это не получится, СББ сразу же зафиксирует BB-атаку, так как протокол LoRa защищен криптоалгоритмом AES128, который злоумышленник не сможет скомпрометировать. Данные, передаваемые через канал USB, не будут совпадать с контрольными данными, переданными через защищенный канал, подсистема безопасности АТМ заблокирует работу банкомата и уведомит службу безопасности банка о том, что происходит атака на банкомат.

Кроме того, по сети LoRaWAN может быть реализован обмен с сервером безопасности для удаленного обновления ПО СББ, например, «Блокиратора» и передачи сессионных криптоключей для шифрования команд, передаваемых по информационным каналам банкомата.

Сеть LoRaWAN, может быть включена в подсистему Авторизации Сервисных служб и Службы инкассации АТМ и обеспечивать процедуру идентификации\аутентификации с использованием бесконтактных идентификаторов с LoRa интерфейсом.

**Вывод.** Несомненным достоинством предложенного технического решения является то, что для построения эффективной защиты банкомата не требуется вся полнота информации о протоколах обмена с периферийными устройствами и о форматах передаваемых сообщений. Отсутствует внедрение в работу АТМ и изменение параметров и алгоритма его работы, при этом вмешательство в информационный обмен системного блока и периферийного оборудования полностью отсутствует, не нарушаются и не изменяются существующие связи и информационные потоки. Для передачи закрытой служебной информации и команд предлагается в составе СББ применять надежный, хорошо защищенный протокол связи LoRa, который позволит повысить степень защиты СББ АТМ.

Это позволяет с уверенностью утверждать, что предложенный способ организации подсистемы безопасности АТМ с использованием защищенного канала передачи закрытых данных, обеспечит эффективную защиту от большинства известных информационных атак на БУС, имеющих функции выдачи и хранении наличных денег.

**Литература**

1. В банкоматах NCR устранены уязвимости, обнаруженные Positive Technologies // URL: https://www.securitylab.ru/news/494980.php

2. Positive Technologies. Сценарии логических атак на банкоматы, 2018. – С. 23.

3. Евсеев С.П., Король О.Г., Гончарова А.И. Радіоелектроніка, інформатика, управління // Построение моделей атак на внутриплатёжные банковские системы, 2010. № 1. – С. 56–66.

4. Зякин А., Кормин В. Способы несанкционированного снятия наличных из банкоматов, виды атак и способы защиты. 2017.

5. Ateam Scientific. IEEE 802.15.4g Stand. 2015. – С. 35.

6. Кумаритова Д.Л., Киричек Р.В. Обзор и сравнительный анализ технологий LPWAN сетей // Информационные технологии и телекоммуникации. 2016. Том 4. – № 4. – С. 33–48.

7. Фомин М.И., Конев В.Н., Жорин Ф.В., Мулейс Р.Б., Тараканов О.В. Возможность осуществления атаки на системы автоматизации на основе уязвимостей Bluetooth-технологий // Спецтехника и связь. 2013. – № 1. – С. 40–42.

8. LoRa Alliance, Inc. LoRaWAN™ 1.1 Specification. 2017. pp 101.

9. Тихвинский В., Коваль В., Бочечка. Г. Технологая LoRa: перспективы внедрения на сетях IoT // Первая миля. 2016. С. 43–49.

10. Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melià-Seguí, Thomas Watteyne Understanding the Limits of LoRaWAN. 2017. p. 7.

*УДК 628.74*

## РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ СИСТЕМ ДЫМОУДАЛЕНИЯ

**Галузо В.Е., Мельничук В.В., Пинаев А.И.**

*Белорусский государственный университет информатики и радиоэлектроники*
*Минск, Республика Беларусь*

При проектировании в соответствии с [1] установок дымоудаления (ДУ) в составе систем противодымной защиты (ПДЗ) в первую очередь определяется весовой, а затем объемный расход удаляемой газодымовой смеси $L_Д$. Значение последнего определяется при нормированном [1] значении температуры удаляемых газов (более $300^0$С) для подбора вентилятора. Кроме $L_Д$ для подбора вентилятора необходимо значение падения давления в сети $P_C$ установки ДУ. Давление $P_C$ рассчитывается в соответствии с [1] с учетом естественного давления газов $P_{EC}$, определяемого разностью удельных весов наружного воздуха и дыма (при температуре более 300 $^0$С) и высотой шахты. При высоте шахты (здания) 50 м $P_{EC} \approx 300$ Па. Это давление вычитается из расчетного давления $P_C$ установки ДУ.

Аэродинамические испытания установок ДУ проводятся при нормальной температуре в помещении (менее 30 $^0$С). При таких температурах удельные веса удаляемого из помещения и наружного воздуха отличаются незначительно и давление $P_{EC}$ составляет единицы Па, и им можно пренебречь. То есть измерения объемного расхода газа, удаляемого установкой ДУ проводятся при давлении в сети отличающегося от проектного значения, а значит производительность вентилятора и объемные расходы будут отличаться, что может привести к тому, что измеренное значение объемного расхода воздуха $L_B$ будет существенно