Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра инженерной психологии и эргономики

На правах рукописи

УДК 654.02:004.056.55

Федорова
Полина Андреевна

ПОВЫШЕНИЕ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ АППАРАТУРЫ ЗАКРЫТИЯ КАНАЛА НА ИНФОКОММУНИКАЦИОННОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ

АВТОРЕФЕРАТ

на соискание академической степени магистра техники и технологии

1-59 81 01 – Управление безопасностью производственных процессов

Магистрантка П.А. Федорова

Научный руководитель
Д.А. Мельниченко, кандидат технических наук, доцент

Заведующий кафедрой ИПиЭ
К.Д. Яшин, кандидат технических наук, доцент

Нормоконтролер
В.С. Гладкая,
ассистент кафедры ИПиЭ

Минск 2019

ВВЕДЕНИЕ

Важной частью безопасности страны является ее информационная безопасность. Проблемы обеспечения информационной безопасности становятся более весомыми и значимыми в связи с переходом на информационные технологии и автоматизированную основу управления процессами. Защита должна носить системный характер, то есть для получения наилучших результатов все разрозненные виды защиты информации должны быть объединены в одно целое и функционировать в составе единой системы, представляющей собой слаженный механизм взаимодействующих элементов, предназначенных для выполнения задач по обеспечению безопасности информации.

Для защиты информации преимущественно используются средства криптографической защиты информации. К средствам криптографической защиты информации относятся технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

С помощью аппаратуры криптографической защиты информация между объектами информация шифруется и передается по сети общего пользования. Для обеспечения качественной передачи информации необходимо, чтобы аппаратура криптографической защиты была на передаче и приеме синхронизирована.

Для повышения безопасности средств криптографической защиты информации нужно обновлять и следить за передачей информации по закрытому каналу в комплексе: аппаратура, программное обеспечение и, конечно, доступ к ним и ключам. При разработке программного обеспечения аппаратуры криптографической защиты очень большое внимание уделяется правильности реализации идентификации и аутентификации. Так как возможно намеренное ослабление криптографических алгоритмов путем передачи неверных или заведомо слабых параметров в сертифицированные продукты, сокращением длин паролей и другой ключевой информации, внесение «закладок» в исходный код для раскрытия секретных параметров. Необходимо отслеживать и обновлять контроль прав доступа к аппаратуре и ключам.

Для повышения надежность аппаратуры криптографической защиты необходимо учесть появление ошибок при передачи информации, так как данная информация передается в зашифрованном виде, то возникающие

ошибки могут привести к потери большого объема информации. Криптографические технологии обеспечивают три основных типа услуг для электронной коммерции: аутентификацию (которая включает идентификацию), невозможность отказа от совершенного и сохранение тайны.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель работы – повысить надежность работы аппаратуры криптографической защиты в сети SDH работающей в условии стресса

Задачи работы:

– проанализировать существующие аппаратно-программные комплексы АКЗ и их тракты обработки информации;

– разработать и обосновать новую структурную схему тракта обработки информации аппаратуры криптографической защиты с целью повышения надежности работы АКЗ;

– разработать рекомендации по повышению безопасности аппаратуры криптографической защиты с учетом расширения функционала аппаратуры.

Объектом данной диссертации является аппаратура криптографической защиты, а так же ее надежность и безопасность.

Предметом для разработки рекомендаций по повышению надежности аппаратуры криптографической защиты является аппаратно-программный комплекс криптографической защиты цифровых потоков «Авангард», предназначенный для криптографической защиты конфиденциальной информации, передаваемой по первичным цифровым каналам Е12 (Е1) со скоростью до 2 Мбит/с.

Областью применения аппаратуры криптографической защиты являются такие объекты как: вооруженные силы, органы внутренних дел, министерства Республики Беларусь и посольства, а также банки.

Приоритетные направления научных исследований. Тема диссертационной работы соответствует пунктам 5 «Информатика и космические исследования» и 13 «Безопасность человека, общества и государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 годы, утвержденных Постановлением Советом Министров Республики Беларусь 12 марта 2015 г. № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Личный вклад соискателя заключается в самостоятельной подготовке рукописи диссертации, подготовке к публикации материалов по теме исследования.

Структура и объем диссертации. Общий объем диссертационной работы составляет 60 страница, из них 55 страницы основного текста, 7 рисунков, 2 таблиц, библиографических список из 33 источников, включая 2 собственные публикации автора.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Аппаратное средство криптографической защиты содержит ряд дополнительных блоков, которые не требуются в программной реализации:

- блок управления криптографическими ключами;
- генератор случайных чисел;
- постоянная и оперативная память;
- блок синхронизации времени;
- устройство хранения и проверки контрольных сумм и хэш-значений.

Использование специализированных шифропроцессоров для вычислений и отдельных блоков идентификации, аутентификации и авторизации (проверки и генерации электронной цифровой подписи) повышает безопасность аппаратуры.

В число основных достоинств аппаратных шифраторов входят следующие:

- гарантия неизменности алгоритма шифрования;
- наличие аппаратного датчика случайных чисел, используемого при создании криптографических ключей;
- возможность прямой (минуя системную шину компьютера) загрузки ключей шифрования в специализированный процессор аппаратного СКЗИ с персональных идентификаторов – носителей типа смарт-карт и «таблеток» Touch Memory (TM);
- хранение ключей шифрования не в ОЗУ компьютера (как в случае с программной реализацией), а в памяти шифропроцессора;
- идентификация и аутентификация пользователя до загрузки операционной системы;
- аппаратная реализация позволяет добиться высокой скорости шифрования данных.

Кроме того, можно отметить ряд достоинств аппаратной реализации, а именно:

- надежность, позволяющая использовать средство криптографической;
- защиты в критичных по надежности узлах автоматизированных систем;
- возможность реализации отдельным блоком, что зачастую позволяет;
- более гибко строить топологию защищенной автоматизированной системы;
- исключение возможности программного повреждения ключей шифрования, что дает гарантию стабильности системы в целом.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация – это

первая линия обороны, «проходная» информационного пространства организации.

В первой главе проведен анализ методов и средств повышения безопасности АКЗ. Рассмотрены основные атаки на криптосистемы и способы их предотвращения.

При проведении активных атак противник может прерывать процесс передачи сообщений, создавать поддельные (сфабрикованные) или модифицировать передаваемые шифрованные сообщения. Эти активные действия называют попытками имитации и подмены соответственно.

Атака по времени – это атака, используемая злоумышленником в сторонних каналах связи, построена на анализе времени, которое необходимо на исполнение криптографического алгоритма. Самый очевидный способ предотвратить временные атаки – смоделировать алгоритм шифрования таким образом, что все производимые вычисления будут исполняться за равное время.

Атака «Человек посередине». Этот метод основан на том, что злоумышленник подключается к каналу передачи данных, тем самым нарушая криптографический протокол. Для предотвращения данной атаки необходимо усиливать системы идентификации, аутентификации пользователей и средства управления доступом.

Атака «полного перебора» — метод решения задачи путем перебора всех возможных вариантов. Сложностью данного метода является количество всевозможных решений данной задачи. Предотвращение атаки «полного перебора». Самым лучшим способом избежать атак полного перебора является правильный выбор параметров эллиптической кривой.

Предотвратить атаки также возможно с помощью правильного выстраивания системы в целом. Использование блока идентификации и аутентификации, системы авторизации (проверки и генерации электронной цифровой подписи), системы контроля доступа, системы управления ключами. Также для корректного функционирования системы защиты аппаратуры и самого криптосредства необходимо проведение сертификационных испытаний и исследований. На примере АПК «Криптозамок» представлен один из способов повышения безопасности АКЗ.

Во второй главе проведен сравнительный анализ аппаратуры криптографической защиты.

После анализа существующих устройств выявлено, что оптимальным решением для реализации комплекса защищенной передачи информации в сетях общего пользования будет программно-аппаратная система. Злоумышленник не может модифицировать устройство шифрования, не получив прямого доступа к нему, а снижение стоимости изделия достигается за счет программного выполнение задач, некритичных к скорости и безопасности.

Обработка информации выполняется на отдельном вычислительном блоке, что в меньшей степени будет оказывать влияние на производительность компьютеров пользователей.

Рассмотрено место оборудования на сети доступа. Проведенный сравнительный анализ различных образцов аппаратуры показал, что указанное оборудование строится по практически одинаковой схеме и выполняет практически одинаковые функции. Приведено описание параметров аппаратуры криптографической защиты различных фирм. Для описания работы АКЗ возят аппаратно-программного комплекса криптографической защиты «Авангард» созданный научно-исследовательским институтом технической защиты информации Республики Беларусь.

Подробно рассмотрена структурная схема АКЗ и тракт обработки информации. На основании этого выявлены недостатки на сети SDH:

1 Ошибки при приеме зашифрованного потока приводят к выходу дешифратора из синхронизма с передающим шифратором. При этом начинается процесс ресинхронизации передающей и приемной стороны, который длится не менее 40 мс, в результате чего теряется более 320 циклов потока Е1.

2 Недостаточный объем входной буферной памяти и неспособность местного генератора подстраиваться к быстрым скачкам фазы входного потока Е1 не позволяют известной АКЗ обеспечивать бесперебойный режим работы на сетях SDH

Эту проблему возможно изменив структуру тракта обработки потока Е1 в АКЗ. Вместо того, чтобы использовать тактовую частоту местного генератора для считывания информации из входной буферной памяти и для тактирования дешифратора, в разрабатываемом устройстве на эти узлы должен подаваться сигнал тактирования от выделителя тактовой частоты (ВТЧ) входного потока Е1. Это будет обеспечивать безошибочность процесса записи-считывания данных из входной буферной памяти и процедуры дешифрации независимо от наличия сдвигов фазы во входном потоке Е1, вызванных выравниванием указателя в вышестоящей аппаратуре SDH.

Будут изменены параметры местного генератора АКЗ – будет введен режим удержания частоты, чтобы исключить срывы его синхронизации при скачках фазы входного сигнала Е1. Скорость перестройки его частоты станет ограниченной, чтобы генератор ведомого мультиплексора успевал отслеживать изменения частоты генератора АКЗ. На рисунке 1 представлена схема тракта обработки информации Е1.

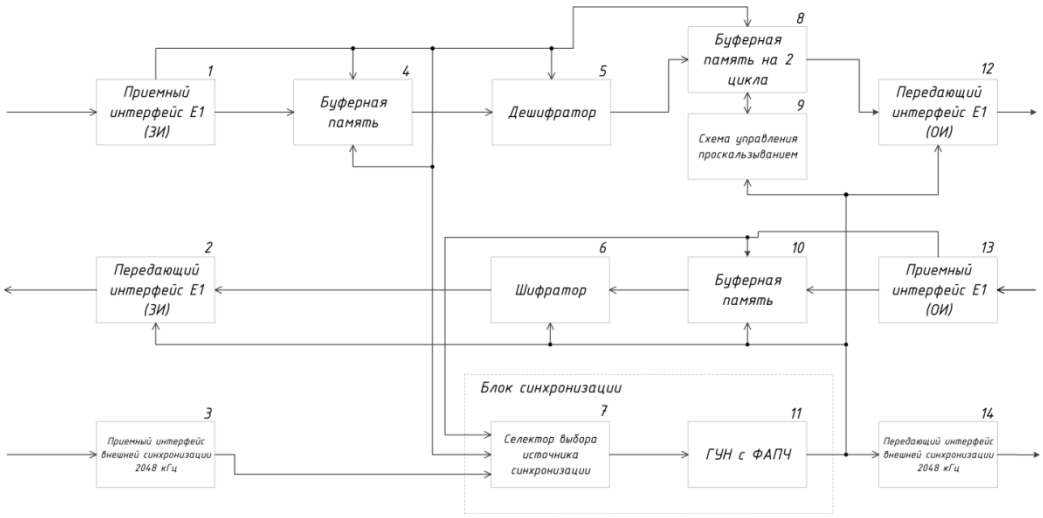

Рисунок 1 – Структурная схема тракта обработки потока Е1 в АКЗ

В третьей главе разработана и обоснована структурная схемы системы АКЗ и блок сихронизации. В новой структурной схеме выходные данные дешифратора с тактовой частотой ВТЧ будут записываться в дополнительную выходную буферную память с объемом 2 цикла Е1 (2х256 бит, т.е. 64 байта) с функцией управляемого проскальзывания, а считываться из нее с помощью тактовой частоты местного генератора. Выходная буферная память позволит скомпенсировать значительные фазовые сдвиги входного потока Е1, а функция управляемого проскальзывания будет обеспечивать предотвращение срывов цикловой синхронизации в нижестоящем первичном мультиплексоре. Изменен местный генератора АКЗ – введен режим удержания частоты, чтобы исключить срывы его синхронизации при скачках фазы входного сигнала Е1. В разработанном блоке синхронизации исключены неуправляемые проскальзывания в потоке Е1 при работе АКЗ, потому что при неуправляемом проскальзывании на 1 бит у существующих АКЗ происходит сбой аппаратуры и потеря ЦСС, приведена его новая структурная схема. Определены рекомендации по повышению безопасности АКЗ.

Повышение безопасности аппаратуры возможно при применении следующих систем и методов:

– двухфакторная аутентификация операторов ПЭВМ до загрузки операционной системы (ОС) с использованием аппаратного идентификатора и пароля, вводимого с клавиатуры ПЭВМ;

– установление подлинности идентификатора оператора с использованием одностороннего протокола строгой аутентификации типа «запрос-ответ» на основе симметричной криптографии (ГОСТ 28147-89);

– разделение полномочий администраторов и пользователей по выбору источника загрузки ОС ПЭВМ, по использованию портов ввода/вывода и

сетевых средств ПЭВМ путем установки и контроля конфигурации настроек BIOS ПЭВМ;

– генерацию случайной числовой последовательности с использованием физического источника шума на полупроводниковых диодах;

– тестирование корректности функционирования устройства, включая самотестирование работоспособности, проверку правильности работы реализованных криптографических функций, контроль качества вырабатываемой случайной числовой последовательности;

– блокирование ПЭВМ при вскрытии корпуса ПЭВМ, предъявлении незарегистрированного в устройстве идентификатора оператора или вводе неверного пароля;

– регистрацию вскрытия корпуса АКЗ и ПЭВМ при включенном и выключенном электропитании ПЭВМ;

– регистрацию в защищенном от несанкционированного изменения журнале событий включения, выключения ПЭВМ, результатов идентификации и аутентификации;

– просмотр и очистку записей журнала событий АКЗ только администратором;

– генерацию криптографических ключей идентификаторов операторов с использованием физического источника шума;

– установку, смену и хранение ключей в зашифрованном виде в энергонезависимой памяти АКЗ, недоступной программным средствам ПЭВМ;

– уничтожение хранимых в энергонезависимой памяти АКЗ ключей при смене ключей, вскрытии корпуса ПЭВМ и/или АКЗ;

– архивирование и хранение администратором ключевой информации для возможности ее последующего восстановления в случае повреждения ключевой информации в АКЗ;

– восстановление ключевой информации только администратором;

– возможность авторизованной замены администратором аппаратных и программных средств ПЭВМ.

ЗАКЛЮЧЕНИЕ

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программнотехнических регуляторов безопасности.

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты – пользователи и процессы могут выполнять над объектами – информацией и другими компьютерными ресурсами. Для сбора и накопления информации о событиях, происходящих в системе и анализ накопленной информации используется протоколирование и аудит.

Исходя из задач данной диссертации, проведен анализ существующих аппаратно-программных комплексов АКЗ и их трактов обработки информации. Были выявлены недостатки работы аппаратуры на сети SDH: ошибки при приеме зашифрованного потока приводящие к выходу дешифратора из синхронизма с передающим шифратором приводят к потери информации и процессу ресинхронизации, так же приводящим к аналогичным последствиям, автоматическое переключение элементов сети SDH на альтернативные источники синхронизации. Для избежание этих проблем предложено изменить структуру тракта обработки потока Е1 в АКЗ. На основе типовой структурной схемы аппаратуры криптографической защиты потока Е1 и структурной схемы тракта обработки потока Е1 разработана новая схема тракта обработки потока Е1 с учетом недостатков, которые присутствуют у известных образцов АКЗ.

Разработаны рекомендации по повышению безопасности аппаратуры криптографической защиты с учетом расширения функционала аппаратуры на основании анализа методов и средств безопасности АКЗ.

Исходя их всего вышеописанного, можно сделать вывод о том, что цель и задачи диссертации, поставленные в введении, выполнены в полном объеме.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Измер, В. Г., Федорова П. А. Системные исследования социотехнических рисков конвергентных технологий / В. Г. Измер, П. А. Федорова, А. Г. Давыдовский // Республиканский конкурс научных работ студентов. – Минск, 2017;

2–А. Федорова, П. А. Анализ способов обеспечения безопасности информации бизнес-структуры (на примере информационно-технической компании) / П. А. Федорова // Студенческий научно-иследовательский проект, Минск – 2019.