Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

На правах рукописи

УДК 004.056

Павловский
Андрей Викторович

ЗАЩИТА ИНФОРМАЦИИ МОБИЛЬНЫХ МАШИН

АВТОРЕФЕРАТ
на соискание степени
магистра техники и технологии

1-59 81 01 Управление безопасностью производственных процессов

Магистрант А.В. Павловский

Научный руководитель
В.В. Савченко, кандидат
технических. наук, доцент

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

Нормоконтролер
Е.С. Иванова, ассистент
кафедры ИПиЭ

Минск 2016

ВВЕДЕНИЕ

Актуальность магистерской диссертации заключается в том, что в настоящее время наблюдается развитие и широкое применение различного рода вычислительных систем во многих сферах человеческой деятельности. Одним из наиболее активно развивающихся направлений этого процесса является разработка и применение ВС на мобильных объектах. Такого рода ВС получили название бортовых цифровых вычислительных систем. БЦВС используются для решения широкого круга задач таких, как сбор, обработка и хранение информации, принятие решений, управление и контроль над работой бортовой аппаратуры. Характерной особенностью условий применения БЦВС является наличие большого количества внешних и внутренних дестабилизирующих факторов (угроз), которые могут негативно воздействовать на информацию в БЦВС. В связи с этим возникает необходимость решения задач связанных с информационной безопасностью БЦВС.

Современная концепция информационной безопасности основывается на идее повышения системности подхода к решению задач защиты информации, суть которого заключается в объединении всех методов и средств, направленных на обеспечение, информационной безопасности, в единый механизм – систему защиты информации. Методы разработки СЗИ представлены в работах: В.А. Герасименко; В.В. Мельникова; В.В. Левкина, А.А. Малюка, В.А. Петрова, А.В. Прелова; S. Castano; М.В. Мецатуняна.

Объектом данного исследования является информационная безопасность мобильного объекта, а предметом – сам ПАК для реализации СЗИ мобильного объекта.

Практическая значимость магистерской диссертации заключается в возможности применять на практике предложенной СЗИ для решения вопросов информационной безопасности мобильных машин путем мониторинга трафика CAN шины.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Объект исследования – информационная безопасность мобильного объекта.

Предмет исследования – ПАК для реализации СЗИ мобильного объекта.

Цель магистерской диссертации – повышение информационной безопасности мобильных машин.

Задачи исследования поставлены следующие:

1. Описать и проанализировать реализуемые механизмы выявление угроз информационной безопасности мобильных объектов.
2. Произвести эргономическое проектирование системы экстренного оповещения пользователя с обоснованием эргономических требований.
3. Провести сравнительный анализ предлагаемого программного комплекса с известными аналогами.

Материалы магистерской диссертации были изложены на 52-й научно-технической конференции студентов, магистрантов, аспирантов БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Задача выявления множества угроз информационной безопасности является одной из главных в проблеме защиты информации БЦВС. Поскольку знание угроз, их типов, источников, а также компонентов системы подверженных угрозам, позволяет обоснованно подойти к выбору или разработке того или иного варианта построения защиты информации.

Для выявления угроз необходимо провести анализ особенностей БЦВС, связанных с их информационной безопасностью. При этом необходимо учитывать как общие особенности вычислительных систем, так и специфические особенности бортовых систем.

ВС представляет собой систему обработки данных, настроенную на решение задач конкретной области применения. В ее состав входят аппаратные и программные средства, используемые для обработки, хранения и передачи информации. Современные ВС характеризуются следующими особенностями, связанными с их информационной безопасностью:

– высокая концентрация информационно-вычислительных ресурсов;

– большая территориальная распределенность компонентов системы;

– интенсивная циркуляция информации между компонентами системы;

– накопление и долговременное хранение больших массивов информации на машинных носителях;

– интеграция в единых базах данных информации различного назначения и различной принадлежности;

– доступ к ресурсам пользователей различных категорий.

На основе специфики CAN интерфейса была предложена СИЗ, алгоритм работы, которой представлена на рисунке 1.1:

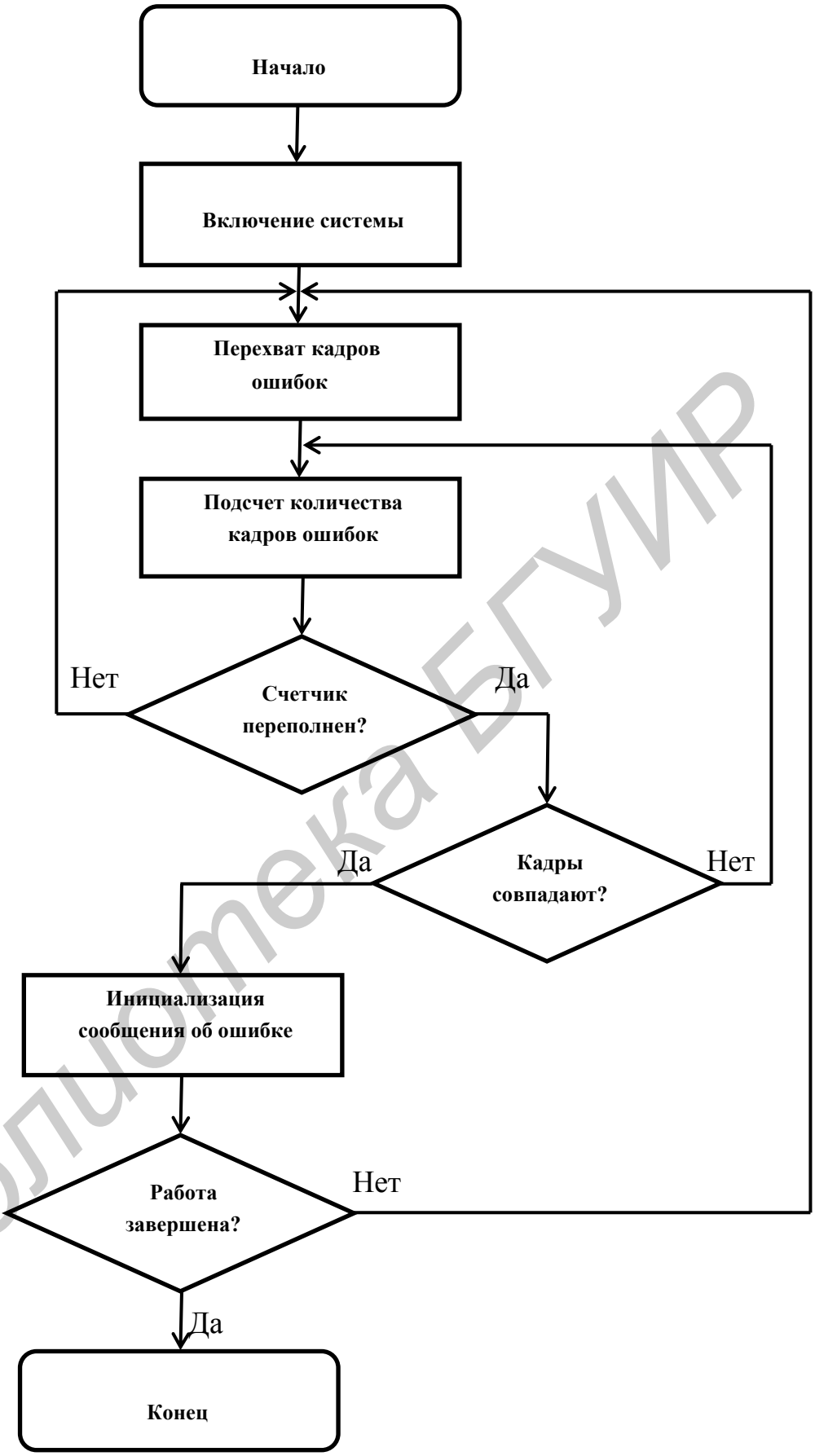

Рисунок 1.1 – Алгоритм работы СЗИ на основе анализа кадров ошибок трафика CAN шины

На основе ГОСТ 21786-76, ГОСТ 21829-76, ГОСТ 22902-78, ГОСТ 12.4.026-76 предложена система экстренного оповещения оператора МО об отказе работы узла CAN.

Данная система совмещает текстовое сообщение «Отказ узла CAN шины», на панели отображения текстовых сообщений МО в зависимости от наличия на МО данной панели, с повторяющимся в интервале 0,2-0,8 с звуковым сигналом, частота которого лежит в диапазоне 800-5000 Гц и уровень звукового давления у входа в наружный слуховой проход оператора, которого лежит в диапазоне 90-100 дБ.

Пример реализации визуальной части экстренного оповещения оператора представлен на рисунке 1.2:

Рисунок 1.2 – Пример реализации визуальной части экстренного оповещения оператор

Предлагаемая СЗИ отличается от известных аналогов тем, что данная система применима к любой системе использующей для канальном уровне протокол CAN. Позволяет не тратя информационные ресурсы системы осуществлять защиту информации МО и выявлять вредоносные узлы, до нанесения ущерба. Это обеспечивает увеличение функциональных возможностей предлагаемой СЗИ по сравнению с известными аналогами в части доступность, простота реализации возможность комбинирования системы с другими СЗИ и средствами обеспечения безопасности оператора МО:

– получение данных о вероятных угрозах информации в системе, с учетом статистики появления сигнатурных кадров ошибки;

– оповещения оператора после выявления угрозы;

– обеспечения разрешения спорных ситуаций в случае возникновения ДТП вследствие выхода из строя систем CAN;

– возможность установки даже МО работающие со старыми версиями протокола CAN;

– защита ПО бортового компьютера путем привязки его к уникальным физическим характеристикам аппаратной части СЗИ.

ЗАКЛЮЧЕНИЕ

Целью магистерской диссертации является повышение информационной безопасности мобильных машин.

Цель магистерской диссертации достигнута.

В ходе проведения исследования были изучены механизмы реализации СЗИ на основе поиска сигнатурных ошибок в трафике CAN шины. Данный метод применим для использования как за счет внутренних ресурсов CAN так и работы за счет ресурсов собственного аппаратного обеспечения СЗИ. Построена блок-схема работы программно- аппаратного комплекса СЗИ и описаны основные этапы работы.

Основные выводы:

1. Проведен анализ особенностей бортовых вычислительных систем, связанных с их информационной безопасностью. В результате анализа были выявлены угрозы информации БЦВС, их типы и источники, а также определены основные направления воздействий угроз. Эта информация позволила обоснованно подойти к разработке схемы построения СЗИ БЦВС, а также к формированию требований к модели защиты информации БЦВС.

2. Определены средства защиты информации, которые могут быть использованы для противодействия выявленным угрозам. Классификация этих средств защиты позволила представить структуру СЗИ БЦВС в виде кортежей средств защиты, принадлежащих мерам защиты законодательного, административного, процедурного и программно-технического уровней. Их использование позволяет осуществлять высокоскоростное закрытие конфиденциальной информации при осуществлении информационного взаимодействия между БЦВС и внешними источниками или приемниками информации.

3. Определены основные эргономические требования предъявляемы к экстренному оповещению оператора об отказе одного из узлов CAN и построена система аварийного оповещения, включающая комбинированный сигнал, состоящий из визуального текстового сообщения и звукового сигнала.

4. В практической части диссертации проведена сравнительная оценка предлагаемой СЗИ с известными аналогами. Результаты оценки показали, что СЗИ в целом удовлетворяет стандартным требованиям, предъявляемым к ПО подобного типа, и способна выявить наиболее опасные злонамеренные действия и отказы узлов. Тем не менее, остается задел для дальнейших усовершенствований, в основном касающихся выявления вредоносных сигнатур способных исполнить свой алгоритм не переполняя счетчик кадров ошибок.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Список использованных источников

[1] Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1. – М.: Энергоатомиздат, 1994. – 400 с.

[2] Ярочкин, В.И. Информационная безопасность. Учебной пособие для студентов непрофильных вузов / В.И. Ярочкин – М.: Междунар. отношения, 2000. – 400 с.

[3] Белов, Е.Б. Основы информационной безопасности: Учебн. Пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия Телеком, 2006. – 544 с.

[4] Бузов, Г.А. Защита от утечки информации по техническим каналам Учебн. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев – М.: Горячая линия - Телеком, 2005. – 416 с.

[5] Спиридонов, О. Б. Разработка модели защиты информации бортовой цифровой вычислительной системы: диссертация кандидата технических наук / О. Б. Спиридонов – Таганрог, 2000. – 255 с.

[6] СТБ 34.101.1-2004 (ИСО/МЭК 15408-1:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

[7] СТБ 34.101.2-2004 (ИСО/МЭК 15408-2:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

[8] СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности»

[9] Кобзарь, М.И. Общие критерии оценки безопасности информационных технологий и перспективы их использования / М.И. Кобзарь, И.И. Калайда // ZJet Info. – 1998. – №1(56). – С. 12-17.

[10] Кобзарь, М.Т. Общие критерии оценки безопасности информационной технологии и перспективы их использования / Кобзарь, М.Т. // Безопасность информационных технологий. – 1998. – №1. – С. 22-24.

[11] Вайнштейн, Л.А. Психология труда : курс лекций / Л.А. Вайнштейн. – М.: БГУ, 2008. – 219 с.

[12] Информационная безопасность и защита информации на железнодорожном транспорте: учебник: в 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте под ред. А.А. Корниенко / Изд-во УМЦ ЖДТ (Маршрут) – 2014 – с.440

[13] Килясханов, И.Ш. Информационное право в терминах и понятиях: учебное пособие / И.Ш. Килясханов , Ю.М. Саранчук // Юнити-Дана – 2012 – 135 с.

[14] Pinker, E.J. Managing Online Auctions: Current Business and Research Issues / E.J. Pinker, A. Seidmann, Y. Vakrat // Management Science Magazine, Volume 49. – 2003. – № 11. – P. 1457–1484.

[15] Спиридонов, О.Б. О динамическом кодировании-декодировании информации / ТРТУ – Таганрог, 1998. – 8 с. – Деп. в ВИНИТИ 1998, № 3284 – В98.

[16] Об экспрессдиверсификации (репликации) информации / Касимов, Ф.Д., Рагимов Р.М., Спиридонов О.Б. и др. // Известия академии наук Азербайджана. – 1999. – №2. – С. 106-110.

[17] Пат. 2130641 РФ, МПК 6G06F 13/00. Способ и устройство защитыинформации от несанкционированного доступа / В.И. Божич, М.Д. Скубилин, О.Б. Спиридонов (РФ). – № 98116168/09; Заявлено 24.08.98; Опубл. 20.05.99. Бюл. № 14.

[18] Пат. 2099890 РФ, МПК 6H04L9/00. Способ шифрования двоичной информации и устройство для осуществления способа – "Албер'ТБ.В. Березин. - № 94014606/09; Заявлено 19.04.94; Опубл. 20.12.97. Бюл.

[19] The Verge [Electronic resource] / Microsoft may halt development work on Silverlight plugin after next release – Vox Media, Inc. – 2011. – Режим доступа: http://www.theverge.com/2011/11/9/2548975/microsoft-may-halt-development-work-on-silverlight-after-next-release. – Дата доступа: 01.05.2016.

[20] Ramchurn, S.D. Trust in Multi-Agent Systems / S.D. Ramchurn, D. Huynh, N. R. Jennings // The Knowledge Engineering Review, Volume 19. – 2004. – № 1. – P. 1 – 25.

[21] Википедия [Электронный ресурс]/ Электронная платежная система – WikimediaFoundation, Inc – 2012. – Режим доступа: http://ru.wikipedia.org/wiki/Электронная_платежная_система. – Дата доступа: 01.05.2016.

[22] WebMoneyWiki [Электронный ресурс] / WebMoney.NETAPI – WMTransferLtd– 2012. – Режим доступа: http://wiki.webmoney.ru/projects/webmoney/wiki/wm-api. – Дата доступа: 01.05.2016.

[23] Показатели качества изделий эргономические. Термины и определения, классификация и номенклатура. ГОСТ 16035-81. – Введ. с 11.08.1982 / М.: Издательство стандартов, 1981. – 5 с

[24] Bonneau, J. The science of guessing: analyzing an anonymized corpus of 70 million passwords / J. Bonneau. – Cambridge: Cambridge University Press, 2012. – 15 p.

[25] Третьяков, С.А. Controller area network (can) - локальная сеть контроллеров / М.: НПКФ «ДЭЙТАМИКРО» – «Электроника» – 1998 – №9-10, – С. 100.

[26] Razgovorov, A., Bykov, M. Система «ЭРА-ГЛОНАСС». Платформа для предоставления услуг // Федеральный сетевой оператор ГЛОНАСС, CEE-SECR 2013 – С. 3.

[27] Bertoni, G. Efficient Software Implementation of AES on 32-bit platforms / G. Bertoni, L. Breveglieri, P. Fragneto. – Berlin: Springer-Verlag, 2003. – 12 p.

[28] Information Technology Secupity Evaluation Criteria. Harmonised Criteria of France-Germany-the Netherlands-the United Kingdom. – London: Department of Trade and Idustry – 1991. – 76 p.

[29] Candian Trusted Computer Product Evaluation Criteria, Version 3.0.

[30] Герасименко В.А. Проблемы создания и организации работы центров защиты информации / В.А. Герасименко // Безопасность информационных технологий. – 1997. – №4. – С. 5-61.

[31] Елисеева И.А., Милославская Н.Г., Петров В.А. Разработка фактографической базы данных по средствам защиты информации и направления ее использования при разработке систем защиты информации // Безопасность информационных технологий. – 1994. – №1. – С. 49-50.

[32] mephi.ru [Электронный ресурс] / «IT-прорыв» – Национальный исследовательский ядерный университет «МИФИ» – 2016 – Режим доступа: https://mephi.ru/special/press/news/1387/60707/ – Дата доступа: 01.05.2016.

Список публикаций соискателя

[1-А] Павловский А.В., Защита информации мобильных машин / А.В. Павловский, В.В. Савченко. – М.: Современные средства связи. – 2016. – С. 105.