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

УДК 004.056:629.33

Козлов Кирилл Сергеевич

Тема:

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА АВТОТРАНСПОРТНЫХ СРЕДСТВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности Методы и системы защиты информации, информационная безопасность 1-98 80 01

Научный руководитель Таболич Татьяна Георгиевна

к.т.н., доцент

_____

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Обоснование актуальности темы магистерской диссертации. Тема магистерской диссертации, посвященной инженерно-технической защите автотранспортных средств от несанкционированного доступа, является важной и своевременной, т.к. угон автомобилей с помощью электронного взлома по-прежнему является ощутимой «головной болью» автовладельцев.

Оценка современного состояния решаемой задачи. Общая компоновка современных автомобилей за последнее столетие не изменилась — это все тот же ящик на колесах, управляемый посредством руля, педалей, рычага переключения передач и приводимый в движение двигателем внутреннего сгорания.

За последние два десятилетия произошла внешне малозаметная революция в системах управления автомобилем — большинство функций контролируются электронными блоками управления. В современном автомобиле представительского класса имеется 50-70 независимых компьютеров, связанных внутренней сетью передачи данных. Программное обеспечение для этих блоков управления может занимать до сотни мегабайт.

Системы управления двигателем, АБС, роботизированной коробкой передач, контроля микроклимата, безопасности, параметров подвески, колес — далеко не весь перечень основных электронных блоков автомобиля. Хотя изначально автопроизводители заботились об увеличении безопасности, сам дизайн электронной системы управления функциями автомобиля создает новую, мощную угрозу безопасности — возможность хакерских атак на электронную начинку.

Задачи и назначение работы. В этих условиях назначение этой работы – разработка комплексов инженерно-технических мероприятий по защите автомобиля от несанкционированного доступа.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований.

Цель работы:

- исследование инженерно-технической защиты автотранспортных средств от несанкционированного доступа.

Задачи:

- Анализ угроз информационной безопасности
- Разработка методов парирования угроз информационной безопасности

Положения, выносимые на защиту. Способ выделения вредоносного программного обеспечения из зараженного файла. Конструкция мощного инвертора электромобиля минимизирующая электромагнитное излучение.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в разработке способов выделения вредоносного программного обеспечения из зараженного файла, а так же разработка конструкции мощного инвертора электромобиля, которая минимизирует электромагнитное излучение. Практическая ценность работы заключается во внедрении результатов исследования в работу СТО ЧУП «СК Мотор».

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на работе и на кафедре ЗИ БГУИР.

Результаты работы опубликованы в:

1-А Дубина С.С., Козлов К.С., Сечко Г.В., Чернецкий А.М. Обеспечение целостности информации в автосигнализации мобильных объектов // Международная науч.-техн. конф., приуроченная к 50-летию МРТИ–БГУИР (Минск, 18–19 марта 2014 года): материалы конф. в 2 ч. – Ч. 1 / редкол.: А. Н. Осипов [и др.]. – Минск: БГУИР, 2014. – 451 с. – С. 384-385.

2-А Садовой В.В., Козлов К.С., Николаенко В.Л., Пачинин В.И. Вспомогательные материалы для заочников, облегчающие перевод патентов США по защите информации // Международная науч.-техн. конф., приуроченная к 50-летию МРТИ–БГУИР (Минск, 18–19 марта 2014 года): материалы конф. В 2 ч. Ч. 2 / редкол.: А. Н. Осипов [и др.]. – Минск: БГУИР, 2014. – 451 с. – С. 417-418.

3-А Козлов К.С., Королёв Я.П. Вспомогательные материалы для заочников иит, облегчающие перевод патентов США по защите информации // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по

направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 22.

4-А Козлов К.С. Организационно-технические способы защиты информации в автомобилях для противодействия угону // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 43.

5-А Козлов К.С. Программно-технические способы защиты информации в автомобилях для противодействия угону // 50-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014. – 78 с. с ил. – С. 44.

6-А Дубина С.С., Козлов К.С., Сечко Г.В., Чернецкий А.М. Борьба с автоугоном с помощью кодграббера // Материалы XX МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014. – С. 271.

7-А Козловский М.М., Козлов К.С. Алгоритм расследования инцидентов в электромобилях, вызванных вредоносным программным обеспечением // Современные тенденции развития науки и производства: сборник материалов Международной научно-практической конференции (23-24 октября 2014 года), в 4-х томах. – Том 1. – Кемерово: ООО «ЗапСибНЦ», 2014 – 196 с. – С. 37-39.

Результаты работы апробированы на 4 (четырех) научно-технических конференциях, в том числе 3 (трех) международных:

- 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.
- Международная науч.-техн. конф., приуроченная к 50-летию МРТИ–БГУИР (Минск, 18–19 марта 2014 года). – Мн.: БГУИР, 2014.
- МНТК «Информационные системы и технологии» (ИСТ–2014), Нижний Новгород (18 апреля 2014 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2014.
- Современные тенденции развития науки и производства: сборник материалов Международной научно-практической конференции (23-24 октября 2014 года), в 4-х томах, 2014.

По результатам апробации на 50-ой научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии доклад отмечен грамотой руководства БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, трех глав и заключения.

В первой главе «Анализ предметной области» описана предметная область, рассмотрены типы автомобилей, подверженных угрозам информационной безопасности и рассмотрена терминология и классификация угроз информационной безопасности. Сделаны выводы.

Во второй главе «Анализ угроз информационной безопасности» описаны угрозы информационной безопасности для традиционных авто, а также для автомобилей с бортовым компьютером и электромобилей. Также рассмотрены электромагнитные излучения в электромобилях. Сделаны выводы.

В третьей главе «Методы парирования угроз информационной безопасности» описано парирование угрозы угона, парирование угрозы «Вирусы и хакерские атаки на транспортные средства» и парирование угрозы ЭМИ в электромобилях. Сделаны выводы.

ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования можно сделать следующие выводы:

✓ В связи со сложностью современных автомобилей всех типов, обслуживаемых на СТО ЧУП «СК Мотор» и наличием большого числа уязвимостей в них, заниматься информационной безопасностью автомобилей необходимо.

Выявлены наиболее значимые угрозы информационной безопасности автомобиля: Угрозы техногенного характера (электромагнитные излучения и наводки) и угрозы, созданные людьми (угроза угона, вирусы и хакерские атаки)

✓ Проведенный анализ угроз ИБ автомобилей различных типов,позволил выявить для парирования наиболее значимые угрозы:

- угрозы угона
- вредоносное программное обеспечение (ВПО);
- несанкционированный доступ, вызванный атаками хакеров;
- ЭМИ, возникающие в мощных инверторах электромобилей

✓ Определены возможные способы парирования угроз информационной безопасности автомобилей:

- Парирование угона способом «Метка»
- Парирование угона способом «Флешка»
- Парирование угрозы угона путём нейтрализации кодграббера.
- Парирование угрозы «Вирусы и хакерские атаки на транспортные средства»
- Парирование угрозы ЭМИ в электромобилях