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

УДК [681.5+625.1(476)]:004.056.5

Зайкина
Ирина Славомировна

Средства и организация разграничения доступа к автоматизированным информационным системам на примере Белорусской железной дороги

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

Научный руководитель
к.т.н., доцент Сечко Г.В.

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

Цели и задачи проводимых исследований. Белорусская железная дорога все чаще сталкиваются с проблемой нарушения параметров защиты информационного и программного обеспечения КИС, связанной с несанкционированными действиями легальных пользователей – сотрудников предприятия.

Белорусская железная дорога ставит задачи усовершенствования механизмов и технологий контроля работы с информационным и программным обеспечением КИС.

Существует ряд систем предотвращения несанкционированного использования информационного и программного обеспечения, но ни одна из них не обеспечивает комплексной защиты ресурсов КИС.

Необходимость обеспечения комплексной защиты информационных и программных ресурсов требует разработки единой, интегрированной в основную информационную среду предприятия, системы, основной задачей которой является предотвращение максимального количества видов «инсайдерских» атак.

Сложность структуры информационного и программного обеспечения КИС Белорусской железной дороги определяет сложность структуры разрабатываемой автоматизированной системы разграничения доступа (АСРД).

Поэтому целью настоящей работы является разработка методики автоматизированного управления многоуровневым доступом к информационным и программным ресурсам Белорусской железной дороги для повышения уровня защиты КИС.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. Белорусская железная дорога все чаще сталкиваются с проблемой нарушения параметров защиты информационного и программного обеспечения КИС, связанной с несанкционированными действиями легальных пользователей – сотрудников предприятия.

Белорусская железная дорога ставит задачи усовершенствования механизмов и технологий контроля работы с информационным и программным обеспечением КИС.

Существует ряд систем предотвращения несанкционированного использования информационного и программного обеспечения, но ни одна из них не обеспечивает комплексной защиты ресурсов КИС.

Необходимость обеспечения комплексной защиты информационных и программных ресурсов требует разработки единой, интегрированной в основную информационную среду предприятия, системы, основной задачей которой является предотвращение максимального количества видов «инсайдерских» атак.

Сложность структуры информационного и программного обеспечения КИС Белорусской железной дороги определяет сложность структуры разрабатываемой автоматизированной системы разграничения доступа (АСРД).

Поэтому **целью настоящей работы** является разработка методики автоматизированного управления многоуровневым доступом к информационным и программным ресурсам Белорусской железной дороги для повышения уровня защиты КИС.

Для достижения поставленной цели в этой диссертации **решены следующие задачи:**

1 Проведение анализа особенностей обработки информации в КИС с точки зрения защиты информационного и программного обеспечения.

2 Разработка методики проектирования автоматизированной системы разграничения доступа КИС для обеспечения должного уровня защиты.

3 Выявление взаимосвязей между структурами Белорусской железной дороги для последующего анализа информационных потоков.

4 Разработка структурной модели автоматизированного управления информационными потоками на Белорусской железной дороге, основанной на принципе контроля и защиты информационного и программного обеспечения КИС.

5 Создание алгоритма управления разграничением доступа сотрудников предприятия к информационным структурам предприятия, объединяющего

процессы идентификации, аутентификации и авторизации сотрудников, целью которого является предотвращение угроз нарушения параметров защиты КИС.

6 Разработка программного модуля управления базой данных автоматизированной системы предприятия с целью обеспечения контроля достоверности ее функционирования.

Положения, выносимые на защиту:

1 Выявленные взаимосвязи информационных ресурсов структурных подразделений Белорусской железной дороге, отличающихся уровнем разграничения доступа к информационному и программному обеспечению КИС.

2 Структурная модель автоматизированного управления информационными потоками Белорусской железной дороги на основе принципов ограничения доступа к ресурсам КИС.

3 Алгоритм управления разграничением доступа в соответствии с должностными инструкциями сотрудников предприятия к информационным структурам предприятия.

4 Основные программно-аппаратные модули автоматизированной системы разграничения доступа к информационному и программному обеспечению КИС.

Теоретическая и практическая значимость. Теоретическая значимость работы заключается в исследовании угроз информационной безопасности информационных ресурсов Белорусской железной дороги и методов их парирования. Научные выводы, представленные в работе, могут быть использованы при проектировании систем защиты информационного и программного обеспечения.

Практическая значимость заключается в методическом обеспечении разработки программно-аппаратного комплекса защиты автоматизированных систем Белорусской железной дороги, основанного на результатах анализа достоинств и недостатков существующих технологических решений.

Связь работы с приоритетными направлениями научных исследований. Тема диссертационной работы соответствует подразделу 5.5 «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 — 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Личный вклад магистранта в выполненную работу. Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на кафедре ЗИ БГУИР и в подразделении Белорусской железной дороги по своему месту работы.

Результаты работы опубликованы в:

Тезисах докл. 50-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии – Основные проблемы информационной безопасности АСУ ТП КВО (Минск, 29 марта 2014 года). – Мн.: БГУИР, 2014.

Материалах XIX Междунар. науч.-техн. конф. «Современные средства связи» – Безопасность информации в АСУТП контроля устройств автоматики, 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014.

Тезисах докл. 51-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии – Основные проблемы информационной безопасности АСУ ТП КВО (Минск, 18 апреля 2015 года). – Мн.: БГУИР, 2015.

Современные средства связи: материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014

Результаты работы апробированы на 5 (пяти) научно-технических конференциях, в том числе 3 (трёх) 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.

XIX Междунар. науч.-техн. конф. «Современные средства связи», 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.].

51-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии – (Минск, 18 апреля 2015 года). – Мн.: БГУИР, 2015.

XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014

По результатам апробации на 50-й и 51-й научных конференциях аспирантов, магистрантов и студентов БГУИР по направлению 8: «Информационные системы и технологии» доклады отмечены благодарностями руководства БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ

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

В первой главе «Исследование и анализ теоретических основ разграничения доступа к информационным и программным ресурсам кис белорусской железной дороги» проведен анализ особенностей обработки информации в КИС с точки зрения защиты информационного и программного обеспечения от внутренних угроз, угроз нарушения параметров защиты информационного обеспечения автоматизированных систем Белорусской железной дороги, путей их предотвращения, причин утечек информационных ресурсов КИС, использования основных методов детектирования информационного контента.

Во второй главе «Постановка задач автоматизированного управления многоуровневым доступом», поставлены основные задачи автоматизированной системы разграничения доступа Белорусской железной дороги согласно методике управления многоуровневым доступом. Решены основные задачи и исследованы дополнительные, решаемые автоматизированной системой разграничения доступа.

В третьей главе «Методика контроля работы с кис на основе разработки применения криптоаналитических методов в технологиях класса DLP» определены архитектуры и инфраструктуры DLP-системы, выделены основные принципы разработанной DLP-системы. Рассмотрены взаимодействие автоматизированных рабочих мест, структур управления и данных в DLP-системе. Выбраны основных критериев функционирования DLP-системы.

В четвёртой главе «Основные аспекты разработки автоматизированной системы разграничения доступа к информационному обеспечению КИС Белорусской железной дорог». Составлена Структурная модель управления предприятием с учетом управления защитой информационного обеспечения КИС. Создан алгоритм работы пользователя с автоматизированной системой разграничения доступа к информационному и программному обеспечению. Разработана структура базы данных предприятия. Рассмотрены связи основных модулей автоматизированной системы разграничения доступа к информационному и программному обеспечению

Разработано программное средство, учитывающее все требования, указанные в данной работе. Средство отлажено, протестировано и пригодно к эксплуатации.

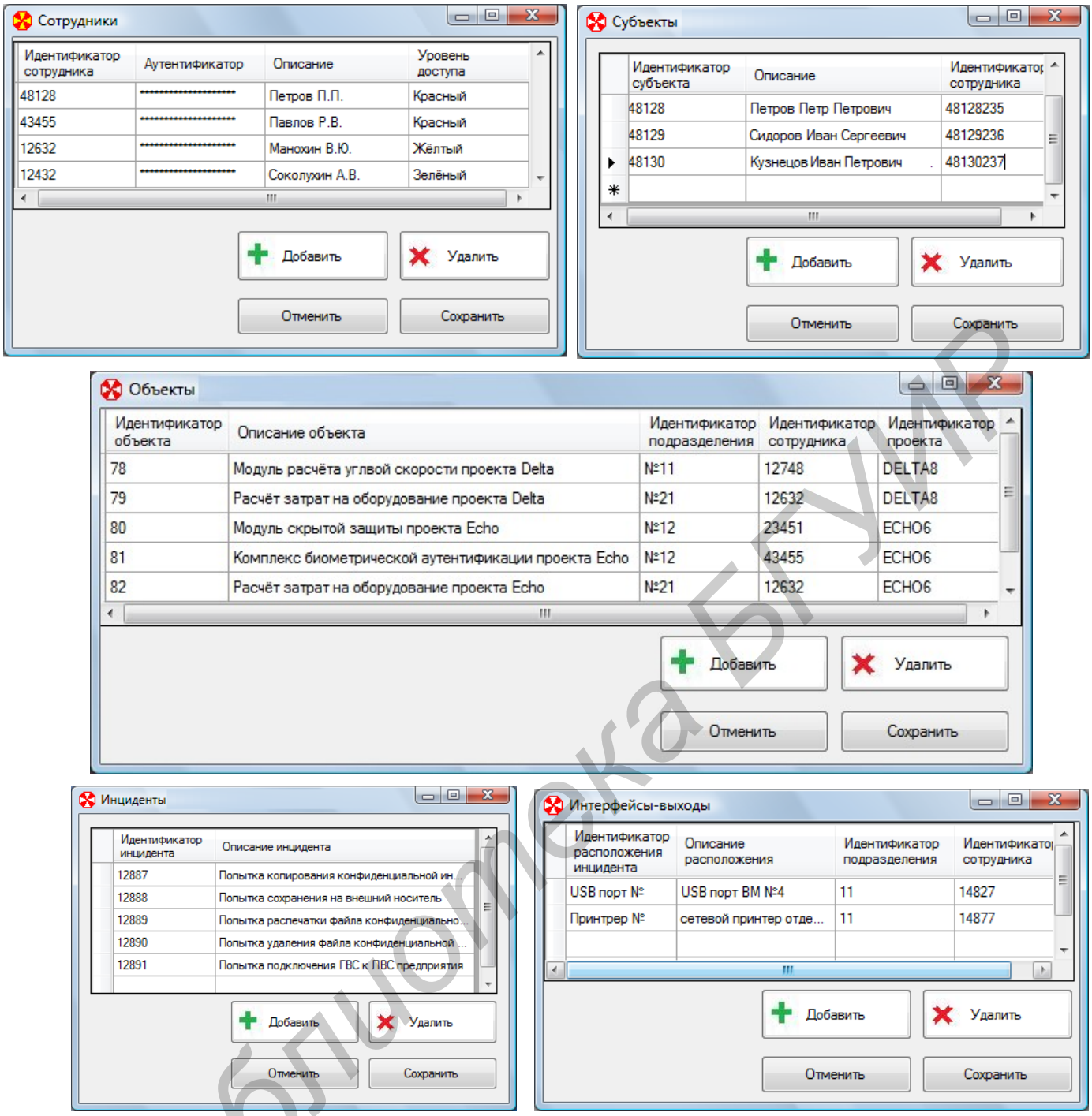

Рисунок 1.1 – Формы работы сотрудников отдела информационной безопасности

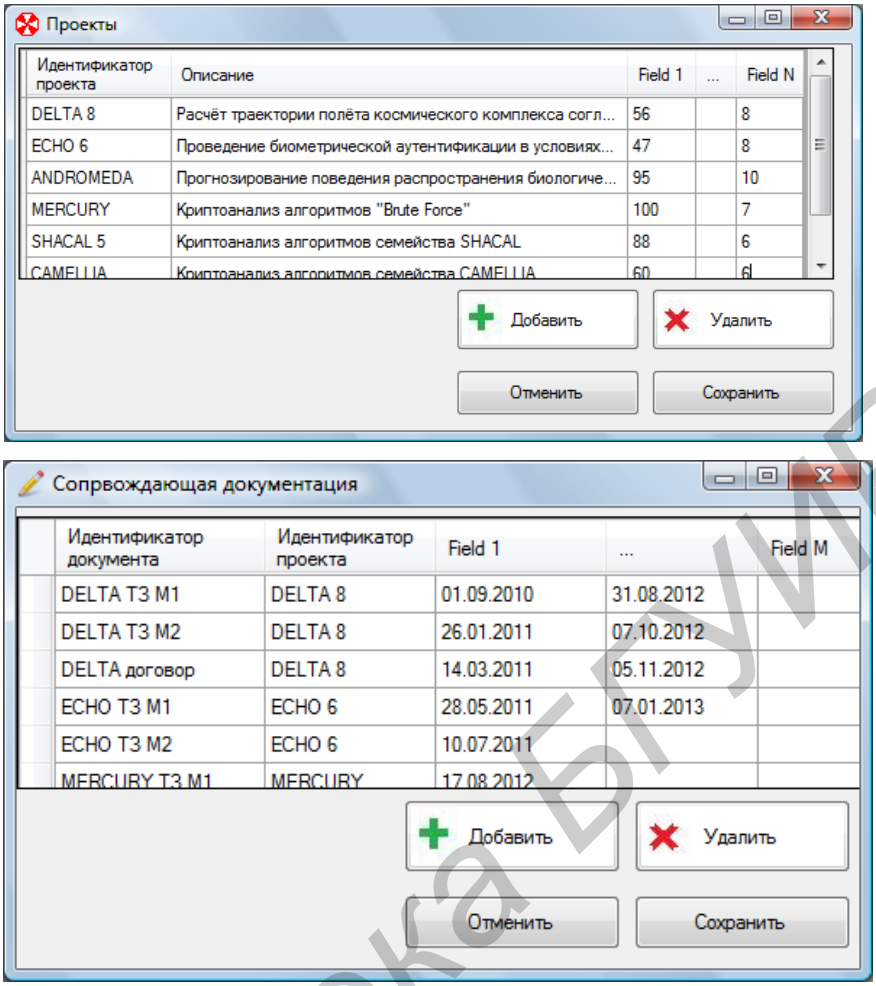

Рисунок 1.2 – Формы работы разработчиков

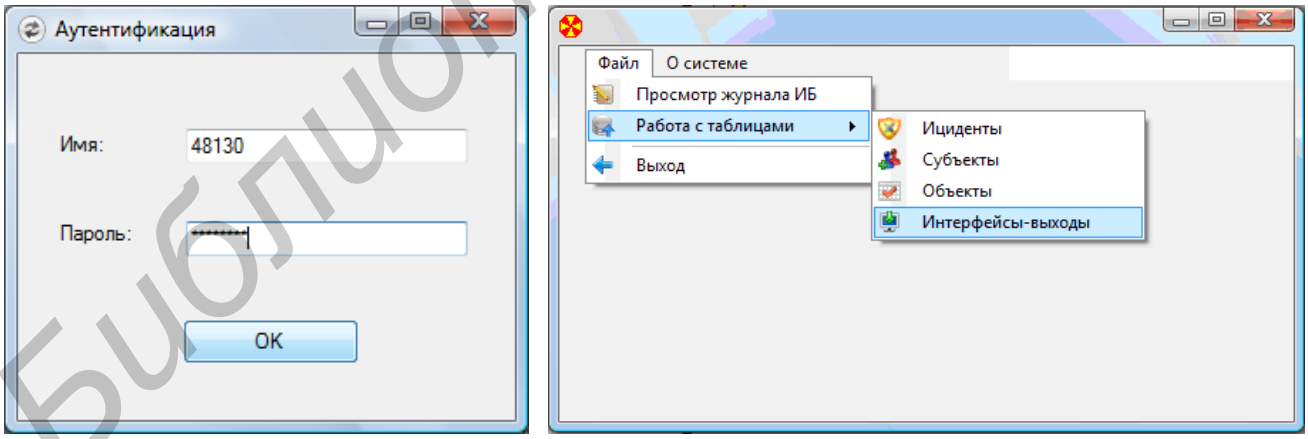

Рисунок 1.3 –Форма аутентификации при входе в систему

ЗАКЛЮЧЕНИЕ

С целью обеспечения должного уровня защиты информационного и программного обеспечения КИС Белорусской железной дороги разработаны методики автоматизированного управления разграничением доступа к стратегически важным информационным и программным ресурсам.

Выявлены взаимосвязи между структурными подразделениями Белорусской железной дороги для последующего анализа информационных потоков.

На основе выявленных взаимосвязей разработана структурная модель автоматизированного управления информационными потоками на Белорусской железной дороги, основанная на принципах защиты информационного и программного обеспечения КИС.

Спроектированы основные модули автоматизированной системы разграничения доступа к информационному и программному обеспечению. На основе анализа в процессе проектирования разработаны методы усовершенствования существующих решений с учетом выявленных основных достоинств и недостатков аналогичных модулей отечественных и зарубежных производителей.

Создан алгоритм управления разграничения доступом сотрудников Белорусской железной дороги к информационным структурам предприятия, включающий процессы идентификации, аутентификации и авторизации сотрудников.

Согласно созданному алгоритму спроектирована база данных предприятия, представлен вариант разграничения доступа к таблицам базы данных сотрудникам структурных подразделений Белорусской железной дороги.

Разработан программный комплекс работы администратора автоматизированной системы с базой данных сотрудников Белорусской железной дороги.

Перспективами дальнейшей разработки темы является расширение областей применения представленной в работе методики обеспечения защиты информационного и программного обеспечения.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Зайкина И.С., Бахур Н.И., Богураев Ю.В. Программное средство для учёта компьютерного оборудования на предприятии // 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. 38.

2–А. Зайкина И.С. Патентование баз данных и компьютерных программ в США и Республике Беларусь // 51-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 18 апреля 2015 года). – Мн.: БГУИР, 2015. – 75 с. с ил. – С. 39-40.

3–А. Зайкина И.С. Защита персональных данных в библиотеке Белорусской железной дороги // 51-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 18 апреля 2015 года). – Мн.: БГУИР, 2015. – 75 с. с ил. – С. 41.

4–А. Зайкина И.С., Сечко Г.В. Повышение информационной безопасности библиотечных баз данных // Современные средства связи: материалы XIX Междунар. науч.-техн. конф., 14–15 окт. 2014 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2014. – 299 с. – С. 211-212.

5–А. Зайкина И.С., Моженкова Е.В. Защита персональных данных в информационной системе библиотек Белорусской железной дороги // Современные средства связи: материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2015. – 326 с. – С. 176-177.