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

УДК 004.056.5

Шалимо
Евгений Игоревич

Обеспечение информационной безопасности системы выдачи заявлений на получение специальных разрешений

АВТОРЕФЕРАТ

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

Научный руководитель
Сечко Георгий Владимирович
кандидат технических наук, доцент

Минск 2018

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цели и задачи проводимых исследований.

В данной диссертации рассматривается один из модулей ERP системы РУП «Белдорцентр» – модуль автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств (далее – модуль). Этот модуль является веб-приложением, поэтому наиболее подвержен атакам различных злоумышленников. В этих условиях целью настоящей работы является дальнейшее повышение информационной безопасности модуля.

Для достижения поставленной цели в этой диссертации поставлены и решены следующие задачи:

– проведен обзор накопленного опыта в области информационной безопасности «Модуль автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств» и сходных с ним;

– выявлены основные угрозы информационной безопасности рассматриваемого модуля, требующие повышения уровня их парирования;

– разработаны собственные новые организационно-программные способы защиты информации в модуле.

Положения, выносимое на защиту:

1. Анализ угроз информационной безопасности «Модуль автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств».
2. Новые организационно-программные способы защиты информации в модуле, позволяющие парировать угрозы по п. 1.

Теоретическая и практическая значимость результатов

Теоретическая значимость работы заключается в теоретическом обосновании способа защиты информации в «Модуле автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств». Практическая ценность выполненной работы заключается в предоставлении способов более безопасного хранения и обработки данных.

Личный вклад магистранта в выполненную работу

Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на кафедре защиты информации БГУИР. Автором проведены работы по разработке и модификации методов защиты информации и реализации программных средств обеспечения информационной безопасности.

Вклад научного руководителя Г. В. Сечко заключается в постановке задач исследования, определении возможных путей их решения и обсуждении полученных результатов.

Все публикации написаны соискателем лично, без соавторов.

Опубликованность результатов диссертации

Результаты работы опубликованы в следующих изданиях:

1. Шалимо, Е. И. Предварительная оценка информационной безопасности системы выдачи заявлений на получение специальных разрешений / Е. И. Шалимо // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 141–145.

2. Шалимо, Е. И. Защита информации в веб-приложении для электронной подачи заявок на получение разрешения для проезда тяжеловесных транспортных средств по автомобильным дорогам / Е. И. Шалимо // Технические средства защиты информации: Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 74.

Апробация результатов диссертации

Результаты работы апробированы на следующих международных научно-технических конференциях:

Постоянно действующий семинар «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016 (под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко) / Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Технические средства защиты информации: XV Белор.-россииск. НТК (Минск, 6 июня 2017 г.).

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Работа состоит из введения, общей характеристики работы, трёх глав, заключения и одного приложений.

В первой главе «Предметная область» проведен краткий обзор предметной области, для которой производится краткий анализ. Так же представлены основные рассматриваемого модуля ERP.

Входе анализа были выделены основные методы, требующие особого внимания при разработке системы безопасности, в условиях постоянно возрастающего числа пользователей, количества пользователей и объемов информации хранящихся документов и проходящих через систему.

Были приведены основные угрозы:

– Угрозы, обусловленные уязвимостями в скриптах;

– Угрозы, обусловленные SQL–инъекциями;

– Угрозы, обусловленные небезопасной авторизацией и аутентификацией;

– Угрозы, обусловленные межсайтовым скриптингом;

– Угрозы, обусловленные похищенными cookie;

– Угрозы, обусловленные небезопасными настройками PHP.

Во второй главе «Анализ уязвимостей и угроз web-приложений» описаны основные алгоритмы реализации методов и механизмов защиты от несанкционированного доступа к данным на основе собственных средств и модификация существующих стандартных методов.

В третьей главе «Анализ инцидентов информационной безопасности» произведено краткое описание среды разработки и описание разработанных программ и способов взаимодействия с ними.

Методами их минимизации и устранения явились разработанные программные средства контроля действий пользователей и системных событий, разграничения прав доступа, оповещения управляющего персонала о критически важных событиях в системе, анализа программного кода на наличие ошибок, а также ролей пользователей.

Разработанные методы позволяет обеспечить более полную и надежную защиту информации от несанкционированного доступа, а также позволяют оповещать о возникновении критических ситуаций и вести журнал выполняемых пользователями действий. Средства управления правами доступа на практике позволяют более гибко и индивидуально настраивать доступ для каждого пользователя.

ЗАКЛЮЧЕНИЕ

Проведенный анализ рассматриваемой в диссертации системы на получение специальных разрешений на участие в дорожном движении тяжеловесных и (или) крупногабаритных транспортных средств показывает, что эта система является:

с одной стороны, «Модулем автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств» ERP-системы государственного предприятия РУП «Белдорцентр»;

с другой стороны, веб-приложением;

с третьей стороны, частью системы электронного документооборота «Электронного правительства».

Каждая из перечисленных ролей системы на получение специальных разрешений на участие в дорожном движении тяжеловесных и (или) крупногабаритных транспортных средств требует индивидуальной защиты информации.

Как показал обзор проанализированных литературных источников, рассматриваемый в настоящей диссертации «Модуль автоматизации процесса оформления специальных разрешений и предоставления дополнительных возможностей грузоперевозчикам по подаче заявлений на проезд тяжеловесных и крупногабаритных транспортных средств» является типичным модулем ERP-системы с веб-приложениями, имеющим множество уязвимостей. Большинство угроз информационной безопасности, вызванных этими уязвимостями, также как и способов их парирования, являются типовыми.

По результатам работы опубликованы статья и тезисы доклада, результаты диссертации обсуждены на двух научно-технических конференциях.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Шалимо, Е. И. Предварительная оценка информационной безопасности системы выдачи заявлений на получение специальных разрешений / Е. И. Шалимо // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 141–145.

2. Шалимо, Е. И. Защита информации в веб-приложении для электронной подачи заявок на получение разрешения для проезда тяжеловесных транспортных средств по автомобильным дорогам / Е. И. Шалимо // Технические средства защиты информации: Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 74.