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

УДК 004.056.53

Волынец
Павел Леонидович

Система защиты от несанкционированного доступа в централизованных автоматизированных системах банковского обслуживания

АВТОРЕФЕРАТ

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

Научный руководитель
Гурский Александр Леонидович
доктор физико-математических наук, профессор

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.

С переходом крупных финансовых организаций на централизованную модель ведения бизнеса появилась острая необходимость в программных комплексах, которые бы обеспечили возможность централизованного хранения данных, круглосуточного доступа к ним и контроля за её сохранностью, конфиденциальностью и неизменностью. Основной целью данной диссертации является разработка актуальных методов и средств защиты информации от несанкционированного доступа в централизованных АБС, а также модификация существующих методов под необходимости конкретного предприятия.

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

- проведен анализ существующих методов защиты информации от несанкционированного доступа;
- выбор и обоснование средств и способов реализации и модификации существующих методов защиты, для увеличения степени безопасности данных;
- реализация выбранных методов встроенными средствами системы Sap for Banking и языка программирования Abap;
- отладка и оптимизация методов действующей системы.

Положения, выносимое на защиту:

1. Система Sap for Banking и язык программирования Abap содержат достаточный объем встроенных средств, позволяющих решить задачу модификации методов защиты информации с учетом особенностей конкретной программной реализации системы управления счетами и платежными операциями финансовой организации.
2. Разработанные методы анализа программного кода и ролей доступа, контроля выполняемых действий в системе, оповещения о критических событиях в системе позволяют повысить степень защиты информации от несанкционированного доступа в централизованной автоматизированной

банковской системе за счет исключения логических ошибок в коде, исключения превышения ролевых полномочий пользователей, своевременной реакции на возникновение критических ситуаций.

Теоретическая и практическая значимость результатов

Теоретическая значимость заключается в теоретическом обосновании методов защиты информации в выбранной системе от несанкционированного доступа. Практическая ценность выполненной работы заключается в предоставлении способов более безопасного хранения и обработки данных в централизованных системах.

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 А. Л. Гурского заключался 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. Волынец, П. Л. Методы защиты информации в системах на основе решений SAP for banking / П. Л. Волынец // Телекоммуникационные системы и сети: материалы 53-й научной конференции аспирантов, магистрантов и студентов (Минск, 2–6 мая 2017 г.). – Минск: БГУИР, 2017. – С. 99.

2. Волынец П.Л. Система защиты от несанкционированного доступа в централизованных автоматизированных банковских системах // Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 44.

Апробация результатов диссертации

Результаты работы апробированы на следующих международных научно-технических конференциях:

53-я Научная конференция Аспирантов, Магистрантов и Студентов, Телекоммуникационные системы и сети. БГУИР 02 - 06 мая 2017 года, Минск, Респ. Беларусь / редкол.: Минск: УО ВГКС, 2017.

XV Белорусско-Российская Научно-Техническая Конференция «Технические средства защиты информации». НИИ ТЗИ 6 июня 2017 г, г. Минск.

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

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

В первой главе «Предметная область и анализ основных угроз информационной безопасности» проведен краткий обзор предметной области, для которой производится анализ и разрабатывались методы защиты от несанкционированного доступа. Так же представлены основные понятия из области безопасности, которые в дальнейшем используется в следующих разделах.

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 и проходящих через систему.

Были приведены основные угрозы, приводящие к несанкционированному доступу к данным:

- ошибки в программном коде;
- некачественная проверка выполняемых разработок;
- получение доступа сверх выполняемых функций;
- злоупотребление правами доступа;
- отсутствие достаточных средств контроля.

Были перечислены основные методы защиты от несанкционированного доступа:

- разграничение систем;
- управление полномочиями;
- журналирование и оповещение;
- анализ полномочий;
- анализ программного кода.

Во второй главе «Методы и средства защиты от несанкционированного доступ» описаны основные алгоритмы реализации методов и механизмов защиты от несанкционированного доступа к данным в АБС на основе собственных средств и модификация существующих стандартных методов.

Описанные методы могут быть успешно реализованы, средствами, предоставляемыми платформой Sap for Banking и возможностями встроенного языка программирования ABAP/4.

В третьей главе «Средства разработки и практическая реализация методов защиты» произведено краткое описание среды разработки и описание разработанных программ и способов взаимодействия с ними.

Основными рассмотренными угрозами были: ошибки в программном коде, получение доступа сверх выполняемых функций, отсутствие достаточных средств контроля.

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.

При условии адаптации под конкретные требования заказчика разработанная система может быть использована и в других кредитно-финансовых организациях Республики Беларусь

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы был проведен анализ современной литературы по теме исследования и выделены основные методы получения несанкционированного доступа к данным в автоматизированных банковских системах и стандартные средства, предоставляемые программным комплексом для их решения.

Проведенный анализ системы на платформе Sap for Banking показал, что при выполнении собственных разработок в системе, стандартные средства контроля, мониторинга и защиты не обеспечивают достаточный уровень безопасности и требуют доработки под конкретные нужды.

Для обеспечения комплексной безопасности данных требуется разработка и доработка методов анализа кода, разграничения прав доступа и системы ролей, методов анализа непротиворечивости ролей, а также системы подробного журналирования и оповещения для критических событий в системе. Краткое описание доработки и разработки указанных методов защиты от несанкционированного доступа представлено во втором разделе.

Разработанные методы проверки, разграничения прав и наблюдения позволяют дополнить существующую систему безопасности и обеспечить большую безопасность данных.

По результатам работы опубликованы статья и тезисы доклада на научных конференциях.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Волынец, П. Л. Методы защиты информации в системах на основе решений SAP for banking / П. Л. Волынец // Телекоммуникационные системы и сети: материалы 53-й научной конференции аспирантов, магистрантов и студентов (Минск, 2–6 мая 2017 г.). – Минск: БГУИР, 2017. – С. 99.

2. Волынец П.Л. Система защиты от несанкционированного доступа в централизованных автоматизированных банковских системах // Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 44.