Федеральное государственное бюджетное учреждение науки

Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

199178, Санкт-Петербург, 14 линия, 39
Телефон: (812)328-33-11
Факс: (812)328-44-50
E-mail: spiiran@iias.spb.su
http://www.spiiras.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

ЗАКЛЮЧЕНИЕ
Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)

Диссертация Биричевского Алексея Романовича «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» выполнена в лаборатории криптологии Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН).

Биричевский А.Р. является специалистом по защите информации, в 2010 году окончил Федеральное государственное бюджетное образовательное учреждение высшего образования «Сыктывкарский государственный университет имени Питирима Сорокина», 30.11.2015 завершил обучение в заочной аспирантуре Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. Биричевский А.Р. работает ведущим инженерном сектора телекоммуникаций и связи отдела информатизации Отделения – Национального банка по Республике Коми Северо-Западного главного управления Центрального банка Российской Федерации.

Справка о сдаче кандидатских экзаменов №14/204 выдана 29.12.2016 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук.

Научный руководитель — Молдовян Николай Андреевич, доктор технических наук, заведующий лабораторией криптологии СПИИРАН.

По результатам рассмотрения диссертации «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» принято следующее заключение:

Оценка выполненной соискателем работы

В диссертационной работе Биричевского Алексея Романовича проанализированы существующие методы и алгоритмы защиты информации в защищенных операционных системах. Были предложены усовершенствованные методы защиты информации в мобильных операционных системах. Разработаны: способ отрицаемого шифрования обеспечивающий существенное повышение производительности алгоритмов ОШ, удовлетворяющих требованию вычислительной неотличимости от вероятностного шифрования основанных на односторонних преобразованиях; способы практического применения высокопроизводительных алгоритмов отрицаемого шифрования в операционных системах; способ применения отрицаемого шифрования для защиты программного обеспечения от статического анализа машинного кода (дизассемблирования); метод противодействия активной отладке программного обеспечения с использованием отрицаемого шифрования для введения ложных веток кода; протокол аутентификации с использованием одноразовых паролей на основе алгебраического алгоритма отрицаемого шифрования.

Проведена апробация предложенных материалов диссертационной работы в учебном процессе кафедры информационной безопасности Института точных наук и информационных технологий Сыктывкарского государственного университета и в компании ООО «Крейф», деятельность которой связана с разработкой перспективных средств защиты информации.

Актуальность и востребованность данной тематики обусловлена тем, что специализированные защищенные операционные системы могут быть применены в широком круге мобильных устройств.

Личное участие соискателя в получении результатов, изложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованных работах.

Представленные к защите результаты получены лично автором:

1. Метод аутентификации пользователей по одноразовым паролям, обеспечивающий защиту от принуждающего несанкционированного доступа.
2. Метод защитного преобразования передаваемой по открытым каналам информации, обеспечивающий защиту от атак с принуждением к раскрытию ключа защитного преобразования.

3. Метод защиты программного обеспечения от активного и пассивного дизассемблирования, существенно повышающий вычислительную трудоемкость дизассемблирования машинного кода.

4. Метод хранения ключей шифрования обеспечивающий возможность сокрытия наличия резервных серий ключей.

Достоверность результатов проведенных исследований.

Достоверность подтверждена аналитическим обзором текущего уровня исследований и разработок в области методов защиты операционных систем, а также апробацией основных научно-практических положений в печатных трудах и на научных конференциях.

Результаты диссертационной работы использованы в производственной деятельности компании ООО «Крейф» и в учебном процессе кафедры информационной безопасности Института точных наук и информационных технологий Сыктывкарского государственного университета на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

Научная новизна полученных результатов.

В ходе работы были разработаны эффективные методы защиты информации в мобильных устройствах телекоммуникационных и информационных систем:

1. Разработан метод аутентификации пользователей, отличающийся использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования.

2. Разработан метод защитного преобразования передаваемой по открытым каналам информации, отличающийся выполнением требования вычислительной неразличимости по шифртексту от вероятностного защитного преобразования.

3. Разработан метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода с помощью псевдовероятностного защитного преобразования машинного кода.

4. Разработан новый метод хранения ключей шифрования, отличающийся выполнением псевдовероятностного защитного преобразования ключей.

Практическая значимость полученных результатов.

Практическая значимость состоит в том, что применение универсальной операционной системы в мобильных устройствах телекоммуникационных и информационных систем, в том числе в системах защиты информации, позволит унифицировать подходы к обеспечению безопасности при разработке таких систем. Данный подход упростит разработку и производство мобильных устройств. Область применения разработанной ОС включает разработку защищенных аутентифицирующих

устройств (токенов, идентификаторов), систем охраны, устройств защиты программного обеспечения, персональных устройств хранения данных (защищенных файловых хранилищ), аппаратных средств для выполнения защитных преобразований данных.

Специальность, которой соответствует диссертация.

Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Полнота изложения материалов диссертации в работах, опубликованных соискателем.

Основные результаты диссертации изложен в 12 публикациях, в том числе, в 3 статьях опубликованы в ведущих рецензируемых журналах, входящих в перечень ВАК, в 3 докладах на международной конференции и 6 докладах на российских конференциях.

Основные результаты диссертации изложены в следующих работах в необходимой полноте:

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в журналах, входящих в перечень ВАК:

1. Березин А. Н., Биричевский А. Р., Молдовян Н. А., Рыжков А. В. Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18-21.
2. Молдовян Н. А., Биричевский А. Р., Мондикова Я.А. Отрицаемое шифрование на основе блочных шифров // Информационно управляющие системы. № 5. 2014. С. 80-86.
3. Биричевский А.Р. Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования // Труды СПИИРАН. СПб.: Наука, 2016. №3. С.128-138.

Другие публикации:

1. Биричевский А.Р. Подход к обеспечению безопасности взаимодействия процессов при разработке операционных систем. Информационная безопасность регионов России (ИБРР-2013). И 74 VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. С. 49-50.
2. Березин А.Н., Биричевский А.Р., Молдовян Н.А. Особенности задачи дискретного логарифмирования по составному модулю как криптографического примитива // Труды VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов

России (ИБРР-2011)». Санкт-Петербург, 26-28 октября. СПб.: СПОИСУ, 2012. С. 104-108.

3. Биричевский А.Р., Мирин А.Ю., Молдовян Н.А. Нетрадиционные приложения блочных шифров // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2011. С. 72-76.

4. Биричевский А.Р., Молдовян Н.А., Рыжков А.В. Отрицаемое шифрование как механизм защиты информации, хранимой на удаленных носителях // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 29-30 ноября 2012, г. Санкт-Петербург / СПб.: ВАС, 2011. С. 77-81.

5. Березин А.Н., Биричевский А.Р., Мондикова Я.А. Отрицаемое шифрование для защиты информации от НСД // 5-я научно-практическая конференция "Информационная безопасность. Невский диалог". Санкт-Петербург, 12-13 ноября 2013 г. / СПб.: «Студия «НП-Принт». С. 21-22.

6. Биричевский А.Р. Отрицаемое шифрование как механизм защиты приложений от отладки // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 21-22 ноября 2013, г. Санкт-Петербург / СПб.: ВАС, 2013. С. 81-85.

7. Биричевский А.Р. Практическое применение алгоритмов отрицаемого шифрования // Информационная безопасность и защита персональных данных: Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VI Межрегиональной научно-практической конференции / под ред. О.М. Голембиовской. – Брянск: БГТУ,2014. С. 17-18.

8. Биричевский А.Р. Отрицаемое шифрование как механизм защиты приложений от отладки // Комплексная защита объектов информатизации и измерительные технологии: сб. науч. тр. Всероссийской науч.-практической конф. с международным участием. 16-18 июня 2014. -СПб.: Изд-во Политех. ун-та, 2014 С. 8-12.

9. Биричевский А.Р. Способ применения отрицаемого шифрования для хранения ключей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. С. 98-99.

Диссертация «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» Биричевского Алексея Романовича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Заключение принято на расширенном семинаре лабораторий информационно-вычислительных систем и технологий программирования, криптологии, проблем компьютерной безопасности. Присутствовало на семинаре 9 чел. Результаты голосования: «за» — 9 чел., «против» — 0 чел., «воздержалось» — 0 чел., протокол № 2 от 12.05.2017.

Заведующий лабораторией
информационно-вычислительных сист
и технологий программирования СПИ
доктор технических наук, профессор ов

199178, Санкт-Петербург, 14-линия В.
тел. (812) 328-08-87, osipov_vasiliy@m

старший научный сотрудник
лаборатории проблем компьютерной бе
СПИИРАН
кандидат технических наук н

199178, Санкт-Петербург, 14-линия В.О
тел. +7-(812)-328-2642, andreych@bk.ru