е ФГБОУ ВО
дарственный
х технологий

ч

ОТЗЫВ

ведущей организации – Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна» – на диссертационную работу Биричевского Алексея Романовича «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

1. Актуальность темы исследования

В настоящее время мобильные устройства информационно-телекоммуникационных систем получили широкое распространение и разработано большое количество программно-аппаратных средств защиты информации, ориентированных на применение таких устройствах. Некоторые из средств защиты информации на аппаратном уровне имеют весьма схожее строение и встраивание в операционную систему механизмов обеспечения информационной безопасности позволяет существенно сократить время и издержки на разработку прикладного программного обеспечения с возможностью его использования в защищенном режиме.

На данный момент в научно-технической литературе имеется большое количество публикаций, посвящённых безопасности операционных систем. Важной научной задачей является повышение эффективности применяемых способов, алгоритмов и методов защиты информации. Диссертация посвящена разработке методов псевдовероятностного защитного преобразования и их применению в подсистеме обеспечения информационной безопасности мобильных операционных систем, что определяет актуальность выполненного исследования.

2. Научная новизна результатов

Новым в диссертационном исследовании является встраивание в мобильную операционную систему функций защиты от принудительных

атак, реализуемых на основе процедуры псевдовероятностного преобразования информации. Разработан новый способ алгебраического псевдовероятностного защитного преобразования (шифрования) и новый алгоритм блочного псевдовероятностного шифрования. При этом под термином псевдовероятностный понимается вычислительно неотличимый от вероятностного. Впервые для защиты от дизассемблирования машинного кода предложено использовать псевдовероятностного шифрования для введения ложных ветвлений исходного кода. К основным научным результатам, полученным автором в диссертационной работе, относятся:

– метод аутентификации пользователей, отличающийся использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования;

– метод защитного преобразования передаваемой по открытым каналам информации, отличающийся выполнением требования вычислительной неразличимости по шифртексту от вероятностного защитного преобразования;

– метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода с помощью псевдовероятностного защитного преобразования машинного кода;

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

3. Достоверность и обоснованность результатов исследований

Достоверность результатов исследования обеспечивается корректным использованием математического аппарата, результатами экпиреметов отсутствием противоречия результатов диссертационной работы и известных результатов затронутой научно-технической области.

Практическая значимость состоит в расширении спектра потенциальных атак, которым представляется возможность противодействовать с использованием разработанной универсальной мобильной операционной системы. При этом применение универсальной (в смысле неспециализированной) 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.

Личный вклад автора присутствует в постановке задач, личном участии в проведении исследований, подготовке материалов к публикации, апробации их на конференциях. В частности, автором

– предложен метод аутентификации пользователей по одноразовым паролям, обеспечивающий защиту от принуждающего несанкционированного доступа;

– предложен метод защитного преобразования передаваемой по открытым каналам информации, обеспечивающий защиту от атак с принуждением к раскрытию ключа защитного преобразования;

– предложен метод защиты программного обеспечения от активного и пассивного дизассемблирования, существенно повышающий вычислительную трудоемкость дизассемблирования машинного кода;

– предложен метод хранения ключей шифрования обеспечивающий возможность сокрытия наличия резервных серий ключей.

4. Полнота опубликованных результатов работы, их соответствие паспорту специальности

Диссертационная работа состоит из введения, списка сокращений, четырех глав, заключения, списка литературы. Объем работы составляет 154 страницы без учета приложений, 38 рисунков и 7 таблиц.

По теме диссертации опубликовано 3 статьи в научно-технических журналах. Из них 3 статьи опубликованы в журналах, которые входят в перечень ВАК («Вопросы защиты информации», «Информационно управляющие системы» и «Труды СПИИРАН»), в которых в должной полноте раскрыты основные положения диссертационной работы.

Основные результаты данной диссертационной работы докладывались и обсуждались на 3 международных и 6 всероссийских конференциях:

– VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2012)» (Санкт-Петербург, 2012);

– VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2013)» (Санкт-Петербург, 2013);

– всеармейская научно–практическая конференция «Инновационная деятельность в Вооружённых силах Российской Федерации» (Санкт-Петербург, 2012);

– всеармейская научно–практическая конференция «Инновационная деятельность в Вооружённых силах Российской Федерации» (Санкт-Петербург, 2013);

– 5-я научно-практическая конференция "Информационная безопасность. Невский диалог". (Санкт-Петербург, 2012);

– VI межрегиональная научно-практическая конференция «Информационная безопасность и защита персональных данных: проблемы и пути их решения». (Брянск, 2014);

– всероссийская научно-практическая конференция с международным участием «Комплексная защита объектов информатизации и измерительные технологии». (Санкт-Петербург, 2014);

– IX Санкт–Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР–2015)» (Санкт-Петербург, 2015).

Тема диссертации, направленность проведенных исследований и полученных результатов соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по п. 1. «Теория и методология обеспечения информационной безопасности и защиты информации», п. 2. «Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида», п. 5. «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет», п. 6. «Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования», п. 11. «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа», п. 13. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Содержание автореферата соответствует основным положениям диссертационной работы. В нем изложены все основные результаты и положения, выносимые на защиту, и дано достаточно полное представление о научно-практической значимости работы.

5. Рекомендации по использованию результатов и выводов

Результаты диссертационной работы рекомендуется использовать в организациях, деятельность которых связана с исследованием и разработкой систем и средств защиты информации, проведением научных исследований и подготовкой специалистов в области информационной безопасности, в частности, в ПАО "Информационные телекоммуникационные технологии" (ПАО Интелтех), АО «Научно-исследовательский институт «Вектор» (АО «НИИ «Вектор»), ФГБУН Санкт-Петербургский институт информатики и

автоматизации Российской академии наук (СПИИРАН), ФГБОУВО Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина) (СПбГЭТУ «ЛЭТИ»), ФГБОУВО «Сыктывкарский государственный университет имени Питерима Сорокина».

6. Замечания по диссертации и автореферату

Из недостатков работы можно отметить следующие:

1. При построении модели нарушителя мобильной операционной системы не проводилась оценка вероятности реализации угроз.

2. Неполно раскрыты сценарии потенциальных реализаций атак с принуждением.

3. Разработанные алгоритмы псевдовероятностного защитного преобразования представляют интерес для защиты от атак с принуждением, однако их применение имеет ограничения из-за недостаточной их производительности;

4. Варианты применения алгоритма Кузнечик, описанного в новом отечественном стандарте блочного шифрования ГОСТ Р 34.12—2015, в разработанной ОС и предложенных процедурах защитного преобразования не рассматриваются, хотя ряду других блочных шифров уделено внимание.

5. Алгоритм, описанный на с. 11 автореферата (с. 82 диссертации) с некоторой конечной вероятностью не выполняет преобразование отдельных знаков исходного текста.

6. В работе и автореферате имеются технические неточности изложения, например:

- на рис. 21 (с. 85) отсутствуют деления и наименование осей;
- на с. 86 указана максимально возможная скорость разработанного алгоритма, при этом не указано какая скорость базового алгоритма была взята за основу.

Отмеченные недостатки носят частный характер и не снижают научной ценности и практической значимости проведенного исследования.

7. Общая оценка диссертационной работы

Диссертационная работа Биричевского А.Р. на тему «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» является законченной научно-квалификационной работой, в которой решена задача расширения функциональности защищенных мобильных операционных систем, имеющая значение для развития методов защиты информации в мобильных устройствах информационно-телекоммуникационных систем. Работа отвечает требованиям п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г. предъявляемым к диссертациям на соискание

ученой степени кандидата наук, а ее автор Биричевский Алексей Романович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Биричевского А.Р. на тему «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем», автореферат и отзыв ведущей организации рассмотрены и одобрены на заседании кафедры интеллектуальных систем и защиты информации (протокол № 2 от 11.09. 2017 г.).

Заместитель заведующего каф
систем и защиты информации,
кандидат технических наук, до . Васильева

Доцент кафедры интеллектуал
систем и защиты информации,
кандидат технических наук Вагнер

Федеральное государственное бю ысшего
образования «Санкт-Петербургск шленных
технологий и дизайна»
Почтовый адрес: Россия, 191186, Санкт-Петербург, ул. Большая Морская, 18
Телефон: (812) 315-74-70
Адрес электронной почты: makvin@mail.ru