«Комплекс средств и технологий обеспечения кибербезопасности автоматизированных банковских систем нового поколения»

Акционерное общество «Научно-производственное объединение «Эшелон»

Авторский коллектив:

1. Марков Алексей Сергеевич – руководитель работы, доктор технических наук, старший научный сотрудник, президент, акционерное общество «Научно-производственное объединение «Эшелон».

2. Жуков Игорь Юрьевич, доктор технических наук, доцент, генеральный конструктор, акционерное общество «Научно-производственное объединение «Эшелон».

3. Греф Герман Оскарович, кандидат экономических наук, президент, председатель правления, публичное акционерное общество «Сбербанк России».

4. Кузнецов Станислав Константинович, заместитель председателя правления, публичное акционерное общество «Сбербанк России».

5. Лебедь Сергей Васильевич, кандидат технических наук, старший управляющий директор по кибербезопасности, публичное акционерное общество «Сбербанк России».

6. Качалин Игорь Федорович, кандидат технических наук, сотрудник, федеральное государственное казенное учреждение «Войсковая часть 43753».

7. Шеремет Игорь Анатольевич, доктор технических наук, профессор, член-корреспондент Российской академии наук, заместитель директора по науке, федеральное государственное бюджетное учреждение «Российский фонд фундаментальных исследований».

8. Зегжда Дмитрий Петрович, доктор технических наук, профессор, профессор Российской академии наук, заведующий кафедрой «Информационная безопасность компьютерных систем», федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

9. Калинин Максим Олегович, доктор технических наук, доцент, профессор кафедры «Информационная безопасность компьютерных систем», федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Повсеместное распространение автоматизированных банковских систем (АБС) нового поколения, предоставляющих финансовые онлайн-сервисы для операций над денежными средствами на основе возможностей Интернет и систем персональной связи, обеспечило существенное повышение качества обслуживания клиентов банков. Однако это же обстоятельство сделало АБС крайне уязвимыми для киберпреступности, использующей открытость указанных сервисов для хищения денежных средств посредством широкомасштабных высокотехнологичных кибератак на ресурсы АБС. По оценкам международных экспертов, только в 2015 году со счетов клиентов банков различных стран киберпреступниками было похищено около 158 млрд. долларов США, что сопоставимо с годовым бюджетом Российской Федерации.

В сложившихся условиях возникла острая необходимость в разработке и внедрении принципиально новых подходов, технологий и средств обеспечения кибербезопасности АБС, способных нейтрализовать растущие киберугрозы.

В рамках решения этой исключительно сложной, многомерной и наукоемкой проблемы авторским коллективом впервые в Российской Федерации разработан и внедрен в АБС нового поколения системообразующий интеллектуальный программно-аппаратный комплекс, обеспечивающий в рамках сквозного информационного процесса интеграцию территориально разнесенных разнородных средств обеспечения кибербезопасности, глубокий многоуровневый комплексный анализ сведений, поступающих от указанных средств, выявление в жестком реальном времени признаков подготовки и осуществления попыток кибермошенничества и кибератак на АБС, а также оперативное управление их применением в условиях массированных криминальных высокотехнологичных воздействий на АБС.

Основой построения указанного комплекса является распределенная интеллектуальная аппаратно-программная среда с распределенной базой знаний, определяющей логику комплексной интеллектуальной обработки «на лету» гетерогенных потоков информации от локальных средств обеспечения кибербезопасности с целью оперативного выявления признаков кибератак и

попыток кибермошенничества, и распределенной базой данных, обеспечивающей непрерывное накопление информации, фиксируемой указанными локальными средствами, для последующего отложенного анализа с целью перманентной адаптации базы знаний к выявляемым технологиям подготовки и осуществления воздействий на АБС.

Наряду с этим разработаны и внедрены:

унифицированный ряд инновационных аппаратно-программных средств обеспечения кибербезопасности АБС в составе комплекса средств межсетевого экранирования, криптомаршрутизатора, системы обнаружения вторжений, однонаправленного шлюза и потокового антивируса;

комплекс технологий и средств контроля защищенности АБС;

комплекс методов и средств безопасного мобильного банкинга;

комплекс методов и средств обеспечения устойчивости АБС в условиях массированных высокотехнологичных системоразрушающих воздействий на их информационную инфраструктуру;

комплекс принципиально новых методов и технологий обнаружения и нейтрализации непреднамеренных и диверсионных дефектов в программных и аппаратных средствах, используемых в АБС;

комплекс методов управления безопасной разработкой программных средств защищенных АБС и обеспечения их технологической безопасности на этапах создания и отладки;

нормативно-методические основы безопасной разработки и внедрения программных средств защищенных АБС и нормативно-правовые документы, регламентирующие организацию работ в этой области, в том числе национальный стандарт ГОСТ Р 56939-2016;

комплекс средств и нормативно-правовых документов, обеспечивающих интеграцию средств обеспечения кибербезопасности АБС с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Предложенные теоретические, системотехнические и информационно-технологические решения обеспечили создание крупнейшего в России и одного из крупнейших в Европе центра управления кибербезопасностью публичного акционерного общества «Сбербанк России» (ПАО Сбербанк). Разработанные средства и технологии внедрены в более чем 30 банках и финансовых корпорациях нашей страны.

Созданная на основе предложенных решений система кибербезопасности крупнейшего в России ПАО Сбербанк обеспечивает непрерывное устойчивое функционирование его корпоративной сети, включающей около 300 тыс. рабочих станций сотрудников, более 80 тыс. банкоматов, около 20 тыс. средств сетеобразования и защиты информации, и бесперебойное обслуживание 137 млн. розничных и 1,1 млн. корпоративных клиентов банка в 22 странах присутствия (в том числе 25 млн. мобильных), ежесуточно выявляя и нейтрализуя более 14 тыс. кибератак и попыток кибермошенничества посредством глубокого многоуровневого комплексного анализа более 0,5 млрд. сообщений об аномальных событиях от локальных объектов. Благодаря этому только в 2017 году было предотвращено хищение денежных средств на сумму 37,9 млрд. рублей и полностью исключены хищения с 240 млн. карточных счетов клиентов банка. Высокая степень защищенности ресурсов и онлайн-сервисов системообразующего для российской экономики и социальной сферы ПАО Сбербанк обеспечивает рост доверия населения к банку и стоимости его бренда, который за 2017 год вырос на 27% и составляет 11,6 млрд. долларов США.

В целях обеспечения высокой эффективности применения внедряемых средств и технологий создана система подготовки и переподготовки высококвалифицированных кадров в области кибербезопасности АБС нового поколения в составе Академии кибербезопасности ПАО Сбербанк, кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации и ряда профильных кафедр других ведущих высших учебных заведений нашей страны.

ПАО Сбербанк определен Центром компетенции по направлению «Информационная безопасность» в рамках программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р.

Основные оригинальные результаты, полученные авторами выдвигаемой работы, отражены в более чем 400 научных трудах, цитируемых в РИНЦ, Web of Science и Scopus, включая 16 монографий, три из которых опубликованы за рубежом. На ключевые технические решения получено более 40 патентов.

Приведенная общая характеристика работы свидетельствует о ее высоком научно-техническом уровне и значительном эффекте от использования ее результатов в национальной банковской сфере и экономике нашей страны.