УДК 004.7.056;002:004.056;004:004.7;004.9;004722

Лаборатория проблем защиты информации: основные результаты деятельности

Дмитриев Владимир Александрович
заведующий лабораторией проблем защиты информации
E-mail: vladdmitr@newman.bas-net.by

Мартинович Татьяна Сергеевна
научный сотрудник лаборатории проблем защиты информации

Лаборатория проблем защиты информации создана в 1996 г. Первым ее руководителем был В. В. Анищенко, с 2016 г. лабораторию возглавляет В. А. Дмитриев. Основными направлениями деятельности и областями научных исследований лаборатории являются:

– разработка теоретических основ методологии обеспечения защиты информации в информационных системах;

– разработка моделей, методов и средств для обоснования требований к информационным системам по информационной безопасности;

– разработка и формирование показателей и требований для национальных стандартов по оценке защищенности;

– разработка методик испытаний защищенных информационных систем;

– аттестация систем защиты информации в реальных условиях эксплуатации информационных систем;

– разработка методов обнаружения атак в информационно-телекоммуникационных системах.

Коллектив лаборатории, 2015 г. Первый ряд (слева направо): Е. П. Максимович, Т. В. Грузд, В. К. Фисенко, В. Б. Алюшкевич, Т. С. Мартинович, А. И. Трубей; второй ряд (слева направо): В. Ю. Скобцов, Н. И. Трухнова, В. Г. Медведева, М. П. Тур, В. А. Дмитриев, С. А. Соломянко; третий ряд (слева направо): Д. С. Ким, Е. А. Пикин

В рамках шести программ Союзного государства, а также государственных программах научных исследований сотрудники лаборатории успешно выполнили работы по заданиям:

1. «СКИФ-Грид» (2007–2010 гг.) – разработка архитектурных принципов построения суперкомпьютеров СКИФ и грид-сетей, теоретических и алгоритмических основ обеспечения их

безопасности, надежности и отказоустойчивости; обоснование принципов построения и создание медицинских диагностических и телемедицинских систем на базе кластерных конфигураций семейства СКИФ.

2. «Космос-НТ» (2008–2011 гг.), задания 1.1, 1.2 «Разработать и реализовать систему контроля надежности и оперативного аудита наземного сегмента Белорусской космической системы дистанционного зондирования Земли» – разработка автоматизированной системы контроля надежности наземного сегмента Белорусской космической системы дистанционного зондирования Земли (БКСДЗ), представляющей собой комплекс программ системы автоматизированного контроля эксплуатационных показателей надежности БКСДЗ; автоматизированной системы оперативного аудита корпоративной сети БКСДЗ, которая обеспечивает системное объединение встроенных в операционные системы средств аудита информационной безопасности вычислительных средств, используемых в составе корпоративной сети БКСДЗ, и способствует обнаружению нарушения дисциплины обмена информацией, хищения информации, потери ее целостности, конфиденциальности и доступности.

3. «Совершенствование системы защиты общих информационных ресурсов Беларуси и России» (2006–2010 гг.), задание «Разработка методических и нормативных документов анализа и оценки безопасности объектов информационных технологий на этапах проектирования и модернизации информационных систем» – разработка экспериментального образца программного комплекса системы автоматизированного анализа и оценки безопасности объектов информационных технологий на этапах проектирования и модернизации, который представляет собой программную реализацию в автоматизированном режиме инструментальных средств для оценки качества профилей защиты и заданий по безопасности, оценки защищенности корпоративной информационной системы по степени соответствия информационной системы заданию по безопасности.

4. «Стандартизация-СГ» (2011–2014 гг.) – разработка стандарта СТБ ECSS-Q-ST-30C-2014 «Космическая техника. Обеспечение качества продукции. Обеспечение надежности» (науч. руководитель – Л. И. Кульбак, отв.исполнитель – А. И. Трубей). Стандарт определяет программу обеспечения надежности и требования к надежности для космических систем, а также требования к надежности для функций, реализованных в программном обеспечении, и требования к осуществлению взаимодействия между аппаратными и программными средствами.

5. «Мониторинг-СГ» (2013–2014 гг.), задания:

1) «Разработать опытный образец программного комплекса системы мониторинга состояния информационной безопасности процессов интеграции и использования космической информации дистанционного зондирования Земли, обеспечивающий мониторинг аппаратных средств, парольной защиты, попыток несанкционированного доступа к циркулирующей информации (ПК СМСИБ)» (отв. исполнитель – В. А. Дмитриев, исполнители – В. К. Фисенко, А. Б. Степанян, А. В. Афанасьев, Е. П. Максимович). В результате выполнения задания был создан опытный образец ПК СМСИБ, реализующий следующие требования к функциональным характеристикам:

– автоматический анализ и обнаружение компьютерных атак на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным;

– отображение обнаруженных атак в веб-интерфейсе консоли управления опытного образца ПК СМСИБ и уведомление администратора безопасности об обнаруженных атаках;

– автоматическое сохранение истории обнаруженных атак для последующего анализа.

Для обнаружения атак использованы сигнатурные методы.

ПК СМСИБ отслеживает события информационной безопасности, фиксируемые: операционной системой автоматизированных рабочих мест пользователей и серверов; системой управления базой данных; межсетевым экраном; коммутационным оборудованием; системой обнаружения атак; антивирусным программным обеспечением, установленным на автоматизированных рабочих местах пользователей и серверах; прикладным программным обеспечением.

2) «Разработать комплекс методик и программных средств для оценки надежности бортовой аппаратуры маломассогабаритных космических аппаратов при ее проектировании, наземных испытаниях и эксплуатации» (отв. исполнитель – В. Ю. Скобцов, исполнители – Д. А. Вятченин, Л. И. Кульбак, Т. С. Мартинович, Д. С. Ким, А. В. Доморацкий, Е. Д. Николаеня). В результате выполнения задания:

– разработаны метод и программный модуль разведочного анализа обучающих телеметрических данных бортовой аппаратуры маломассогабаритных космических аппаратов (БА МКА);

– разработан экспериментальный образец комплекса методик и программных средств оценки надежности (КМПС ОН БА МКА) в составе:

методики и программного модуля интервальной оценки показателей надежности БА МКА;

программного модуля визуализации структурных схем надежности;

методики и программного модуля интеллектуального анализа данных о состоянии БА МКА;

методики и программного модуля логико-вероятностной оценки надежности БА МКА;

программного модуля визуализации результатов интеллектуального анализа данных;

программного модуля импорта-экспорта телеметрических данных о состоянии БА МКА;

программного модуля разведочного анализа обучающих телеметрических данных (как субмодуля программного модуля интеллектуального анализа данных о состоянии БА МКА);

методики моделирования тепловых и механических воздействий на функциональные элементы БА МКА;

– осуществлена интеграция веб-версии экспериментального образца КМПС ОН БА МКА в программно-моделирующий комплекс многокритериального оценивания, анализа и прогнозирования значений показателей надежности и живучести БА МКА с учетом факторов космического пространства, а также управления их реконфигурацией на различных этапах жизненного цикла программно-моделирующего комплекса, разработанного в Санкт-Петербургском институте информатики и автоматизации РАН.

6. «СКИФ-НЕДРА» (2015–2018 гг.), задание «Разработать методологическое, программное, информационное, нормативно-правовое обеспечение информационной безопасности высокопроизводительных информационно-вычислительных технологий обработки геолого-геофизических данных и систему управления информационной безопасностью» (отв. исполнитель – В. А. Дмитриев, исполнители – В. К. Фисенко, А. Б. Степанян, Д. С. Ким, Е. П. Максимович, Т. С. Мартинович, Н. А. Чуприс). Проведены работы по проектированию, созданию и аттестации системы защиты информации информационной системы обработки геолого-геофизических данных на базе высокопроизводительных информационно-вычислительных технологий в соответствии с требованиями Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62.

Межгосударственная программа инновационного сотрудничества государств – участников СНГ на период до 2020 года (2015–2020 гг.) – выполнены ОКР «Развитие инфраструктуры суперкомпьютерных центров в интересах инновационного развития государств – участников СНГ» (отв. исполнитель – В. А. Дмитриев, исполнители – В. К. Фисенко, А. Б. Степанян, Д. С. Ким, Е. П. Максимович, Т. С. Мартинович, Н. А. Чуприс); работы по проектированию, созданию и аттестации системы защиты информации грид-системы в соответствии с требованиями Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

Государственная комплексная программа научных исследований «Инфотех» (2006–2010 гг.), задания:

1) «Разработка экспериментального программного комплекса систем поддержки принятия решений для защиты информации от сетевых атак в реальном масштабе времени» – разработан экспериментальный программный комплекс системы поддержки принятия решений для защиты информации от сетевых атак в реальном масштабе времени.

2) «Разработка экспертной автоматизированной системы поддержки принятия решений при оценке безопасности объектов информационных технологий, качества профилей защиты и заданий по безопасности» – разработаны экспертная автоматизированная система поддержки принятия решений по оценке качества профилей защиты и заданий по безопасности и эксперт-

ная автоматизированная система поддержки принятия решений по оценке соответствия объектов информационных технологий заданию по безопасности.

Государственная комплексная программа научных исследований «Космические исследования» (2014–2015 гг.), задание «Исследовать и разработать методологические, нормативные и организационные основы обеспечения информационной безопасности наземного сегмента Белорусской космической системы дистанционного зондирования Земли».

Государственная программа научных исследований «Информатика и космос, научное обеспечение безопасности и защиты от чрезвычайных ситуаций», подпрограмма «Информатика» (2014–2015 гг.), задание «Исследование методологических основ новых версий международных стандартов и нормативно-технических правовых актов в области информационной безопасности и разработка программного комплекса аттестации систем защиты информации информационных систем» (науч. руководитель – В. А. Дмитриев, исполнители – В. К. Фисенко, А. В. Афанасьев, А. Б. Степанян, Н. С. Захаревич, Е. П. Максимович, Т. С. Мартинович). Разработаны программный комплекс оценки полноты и качества исходных данных по аттестации систем защиты информации и программный комплекс аттестации систем защиты информации информационных систем.

Государственная программа научных исследований «Информатика и космос, научное обеспечение безопасности и защиты от чрезвычайных ситуаций», подпрограмма «Космические исследования» (2014–2015 гг.), задание «Разработка адаптивных технологий проектирования и применения средств противодействия угрозам геоинформационным системам в базисе самообучающегося нечеткого классификатора» (науч. руководитель – Д. А. Вятченин, исполнитель – А. В. Доморацкий). В результате выполнения задания:

– предложены модель и методика анализа и оценки рисков информационной безопасности корпоративной сети БКСДЗ;

– разработаны специальные лингвистические ресурсы – экспертные правила и алгоритм преобразования «фонема – аллофон», генерирующий лингвистические ресурсы «слово-аллофонная запись», что позволяет эксперту корректировать работу двуязычного синтезатора речи при выявлении ошибок в обработке сверхбольшого множества текстовых запросов без привлечения инженера-программиста при синтезе белорусской или русской речи по сверхбольшому множеству текстовых запросов при возникновении угроз безопасности данным в корпоративной сети БКСДЗ;

– разработана методика прототипирования систем нечеткого вывода в случае тринаправленных обучающих данных, позволяющая производить классификацию объектов в условиях изменения их характеристик под воздействием внешней среды;

– разработана методика формирования обучающей выборки для систем обнаружения вторжений на основе базы KDD’99;

– разработаны алгоритмы построения лингвистических ресурсов для идентификации количественных выражений с единицами измерения СИ, производными от СИ и вне СИ для текстового процессора синтезатора речи, который будет использован при озвучивании текстовых данных с количественными выражениями в системе при возникновении угроз безопасности.

Государственная программа научных исследований «Информатика, космос и безопасность», подпрограмма «Информатика и космические исследования» (2016–2020 гг.), задания:

1) «Исследование и развитие процессного подхода к оценке и обработке рисков информационной безопасности продуктов и систем информационных технологий и их классификации по уровням безопасности» (науч. руководитель – В. А. Дмитриев, исполнители – В. К. Фисенко, Е. П. Максимович, А. Б. Степанян, В. Ю. Скобцов, Т. С. Мартинович, Д. С. Ким, Н. А. Чуприс). В результате выполнения задания разработаны:

– программный комплекс автоматизации процесса оценки и обработки рисков информационной безопасности продуктов и систем информационных технологий, который позволяет идентифицировать и классифицировать угрозы, уязвимости и риски, оценивать вероятности реализации угроз, уязвимостей и рисков, идентифицировать меры защиты, оценивать возможные последствия;

– алгоритмы обнаружения дефектов модулей программных средств на основе применения алгоритмов мягких вычислений и метаэвристик с целью уменьшения рисков нештатного функционирования программных модулей.

2) «Управление доступом к ресурсам распределенных информационных систем на основе отношений доверия с учетом механизмов централизации и децентрализации» (науч. руководитель – В. А. Дмитриев, исполнители – Е. П. Максимович, А. Б. Степанян, В. Ю. Скобцов, Т. С. Мартинович, Д. С. Ким, Н. А. Чуприс). Разработан программный комплекс управления доступом к ресурсам распределенных информационных систем на основе отношений доверия с учетом механизмов централизации и децентрализации, содержащий:

– программное средство управления логическим разграничением доступа субъектов к объектам сложных централизованных распределенных информационных систем путем использования отношений доверия;

– программное средство управления и защиты ресурсов распределенных децентрализованных информационных систем с элементами централизации или без таковых на основе алгоритмов консенсуса, алгоритмов хеширования и криптозащиты с возможностью поддержки смарт-контрактов или элементов криптохранилищ.

Программный комплекс обеспечивает:

– запуск и доступности всех компонентов меню генератора сети;

– выполнение полной установки компонентов сети: проверку и установку предварительных условий, проверку и установку компонентов HF (Hyperledger Fabric), установку компонентов HF;

– генерацию сети по заданным параметрам;

– установку инструментов разработчика CC (Chain Code) – VS (Visual Studio) Code;

– запуск и самотестирование сети, сгенерированной по заданным параметрам с тестовым и основным CC.

Государственная программа научных исследований «Цифровые и космические технологии, безопасность человека, общества и государства», подпрограмма «Цифровые технологии и космическая информатика» (2021–2025 гг.), задание «Поведенческие и интеллектуальные методы обнаружения атак в телекоммуникационных сетях» (науч. руководитель – В. А. Дмитриев, исполнители – В. Ю. Скобцов, Е. П. Максимович, Т. С. Мартинович, А. Ю. Квач). Разработаны статистические, спектральные, фрактальные, параметрические методы обнаружения атак, методы вейвлет-анализа обнаружения атак, гибридная нейросетевая модель обнаружения атак с использованием методов машинного обучения.

Поведенческие и интеллектуальные методы обнаружения атак будут использованы при разработке программного комплекса обнаружения атак.

Государственная научно-техническая программа «Защита информации» (2006–2010 гг.), задания: ОКР «Экран-1», ОКР «Доступ», НИР «Модель», ОКР «Мониторинг». В результате выполнения заданий:

– разработаны научно-методологические основы комплексной защиты информации;

– создан межсетевой экран для безопасного подключения локальной вычислительной сети к открытым вычислительным сетям;

– создана система контроля и обнаружения удаленных сетевых атак;

– разработан аппаратно-программный комплекс средств защиты информации от несанкционированного доступа с применением средств криптографии;

– разработан комплекс моделей синтеза и анализа требований безопасности информационных технологий.

Государственная научно-техническая программа «Защита информации-2» (2011–2015 гг.), задание «Разработать технические нормативные правовые акты и методические документы для проведения аттестации систем защиты информации» (отв. исполнитель – Е. П. Максимович, исполнители – В. К. Фисенко, Т. С. Мартинович). В результате выполнения задания разработаны:

– СТБ 34.101.1-2014 (ISO/IEC 15408-1: 2009) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;

– СТБ 34.101.2-2014 (ISO/IEC 15408-2: 2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;

– СТБ 34.101.3-2014 (ISO/IEC 15408-3: 2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности;

– типовые методики оценки качества профилей защиты и заданий по безопасности, разработанных в соответствии с требованиями стандартов СТБ 34.101.1-2014 – СТБ 34.101.3-2014;

– типовые методики испытаний функций безопасности продуктов информационных технологий.

Вышеуказанные стандарты являются базовыми в области оценки безопасности информационных технологий и гармонизированы с международными стандартами. На их основе предъявляются требования безопасности к продуктам информационных технологий. В стандартах излагается концепция оценки безопасности продуктов информационных технологий, содержатся каталоги функциональных и гарантийных требований безопасности, используемые для разработки профилей защиты и заданий по безопасности, а также для оценки защищенности продуктов информационных технологий.

Разработанные стандарты используются при разработке профилей защиты и заданий по безопасности, испытании продуктов информационных технологий, составлении экспертных заключений и выдаче сертификатов соответствия.

В каждой из методик определены:

– совокупности проверок, которые должен выполнить эксперт для всестороннего и полного анализа профилей защиты и заданий по безопасности, проведения испытаний функций безопасности объекта оценки на соответствие профилей защиты и заданий по безопасности определенного уровня гарантии;

– комбинированные (лингвистические и соответствующие им интервальные) шкалы оценок, используемые экспертом для выставления оценок при проведении установленной совокупности проверок;

– правила формирования обобщенных количественных оценок по совокупности выставленных экспертом оценок;

– правила принятия решения о результатах оценки качества профилей защиты и заданий по безопасности, испытаний функций безопасности объекта оценки на соответствие профилей защиты и заданий по безопасности определенного уровня гарантии на основе обобщенных количественных оценок.

Публикации

Сотрудниками лаборатории опубликовано более 300 научно-технических статей и докладов по направлениям деятельности лаборатории, в том числе монографии:

1. Медицинские информационные системы и технологии / С. В. Абламейко, В. В. Анищенко, В. А. Лапицкий, А. В. Тузиков. – Минск : ОИПИ НАН Беларуси, 2007. – 176 с.

2. Вятченин, Д. А. Нечеткая кластеризация и нечеткая математическая морфология в задачах обработки изображений / Д. А. Вятченин, А. В. Хижняк, А. В. Шевяков. – Минск : ВА РБ, 2012. – 271 с.

3. Вятченин, Д. А. Нечеткие методы автоматической классификации / Д. А. Вятченин. – Минск : УП «Технопринт», 2004. – 219 с.

4. Viattchenin, D. A. A heuristic approach to possibilistic clustering: algorithms and applications / D. A. Viattchenin. – Berlin : Springer-Verlag Berlin, 2013. – 227 p.