Форма 501. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1 Номер проекта

13-01-00843

1.2 Руководитель проекта (фамилия, имя, отчество)

Котенко Игорь Витальевич

1.3 Название проекта

Математические модели и методы мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающиеся на интеллектуальных сервисах защиты информации

1.4 Код и название конкурса

А Инициативный

1.5 Год представления отчета

2014

1.6 Вид Отчета (2 - этап 2014 г.)

2

1.7 Аннотация (не более 1 стр.; описать содержание фактически проделанной работы и полученные результаты за 2014 год)

Выполнено уточнение и доработка формальных моделей и программных прототипов компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности и определения рисков безопасности информации, верификации политики безопасности, активного аудита и защиты информационных и программных ресурсов от вредоносного программного обеспечения. Выполнена теоретическая и экспериментальная оценка предложенных решений. Получены свидетельства о государственной регистрации программ для ЭВМ для вычисления показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности, формирования модели нарушителя для анализа защищенности информационно-телекоммуникационных систем, верификации сетевых информационных потоков для защиты информационно-телекоммуникационных систем со встроенными устройствами, поддержки принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи, решения задачи оценки и прогнозирования состояния распределенных информационных систем.

1.8 Полное название организации, предоставляющей условия для выполнения работ по Проекту физическим лицам (использовать только официально утвержденное название)

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Форма 503. РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1 Номер проекта

13-01-00843

3.2 Название проекта

Математические модели и методы мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающиеся на интеллектуальных сервисах защиты информации

3.3 Коды классификатора, соответствующие содержанию фактически проделанной работы (в порядке значимости)

01-217, 01-202, 01-216, 07-235, 07-241

3.4 Объявленные ранее цели проекта на 2014 год

Основные цели проекта на 2014 год были связаны с продолжением работ по разработке, прототипированию, теоретической и экспериментальной оценке моделей и методов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающихся на интеллектуальных сервисах защиты информации, в частности, гибридного многоагентного моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей, анализа рисков безопасности информации, верификации политики безопасности, активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения.

Ставились следующие задачи: 1) уточнение и доработка формальных моделей и программных прототипов компонентов исследовательского моделирования компьютерных атак и процессов защиты от них; 2) уточнение и доработка формальных моделей и программных прототипов компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации; 3) уточнение и доработка формальных моделей и программных прототипов компонентов верификации политики безопасности; 4) уточнение и доработка формальных моделей и программных прототипов компонентов активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения; 5) продолжение исследований по теоретической и экспериментальной оценке предложенных моделей и методов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур.

3.5 Степень достижения поставленных в проекте целей

Все задачи, запланированные в проекте на 2014 год, выполнены полностью. Уточнены и доработаны формальные модели и программные прототипы компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности и определения рисков, верификации политики безопасности, активного аудита, а также продолжены исследований по теоретической и экспериментальной оценке предложенных решений.

3.6 Полученные в 2014 году важнейшие результаты

1. Уточнены и доработаны формальные модели и программные прототипы компонентов исследовательского моделирования компьютерных атак и процессов защиты от них.
Уточненные модели, методики и прототипы основаны на построении и анализе графов атак, позволяющих, с одной стороны, оценить защищенность компьютерной сети от атак, а с другой – участвовать в анализе событий безопасности для выявления наиболее вероятных трасс атак и, как следствие, наиболее вероятных нарушителей. Основной особенностью, отличающей предложенные модели и методики от существующих, является способ использования графов атак и учета текущих событий безопасности для идентификации фрагмента графа атак.
На этапе подготовки к построению деревьев атак для каждого хоста строится трехмерная матрица по следующим данным: класс атак (сбор данных, подготовительные действия, повышение привилегий, выполнение цели атаки); необходимый тип доступа (удаленный источник без прав

доступа, удаленный пользователь системы, локальный пользователь системы, администратор); уровень знаний нарушителя (типы уязвимостей, которые нарушитель может реализовывать).
В результате, для каждого хоста формируется список возможных атакующих действий, разбитых на группы по следующим параметрам: класс атаки, необходимый тип доступа и необходимый уровень знаний нарушителя, а для каждой группы, в свою очередь, формируется список конкретных атак и уязвимостей, которые эти атаки используют. Общий список уязвимостей формируется на основе описания программно-аппаратного обеспечения хоста на языке Common Platform Enumeration (CPE) и таких открытых баз уязвимостей, как National Vulnerability Database (NVD). Источниками данных об открытых уязвимостях также могут служить отчеты сканеров безопасности, таких как Nessus, MaxPatrol и др. Уязвимости в системе хранятся в формате Common Vulnerabilities and Exposures (CVE). Кроме отдельных уязвимостей при построении графа атак используются шаблоны атак в формате Common Attack Pattern Enumeration and Classification (CAPEC), которые могут выступать не только в качестве входной информации для построения графов атак, но и как результат анализа безопасности – они могут описывать наиболее часто встречающиеся последовательности эксплуатации уязвимостей и других действий атакующего.
После формирования матрицы потенциальных атак для каждого хоста, для анализируемой сети выбираются возможные типы нарушителей и точки доступа, в которых они могут получить доступ к сети.
Далее для каждой выбранной модели нарушителя составляется список возможных целей. Так, для внутреннего пользователя это может быть месть (то есть причинение максимального ущерба компании), для внешнего хакера это может быть доступ к некоторой конфиденциальной информации, расположенной на определенном сервере внутри сети, а для червя целью может быть распространение инфекции по сети.
Соответственно, моделью нарушителя для конкретной сети является множество пар (тип нарушителя, цель), которые определяют ограничения по использованию атакующих действий и возможные начальные точки доступа в сеть. После этого на основе собранной информации формируются графы атак для всех выбранных моделей нарушителя.
В режиме обработки событий безопасности основная функция системы защиты информации – выявление конкретных нарушителей и формирование направленной защиты.
Предлагаемый подход использования графов атак для обнаружения атак, проводимых в реальной сети, содержит три основных этапа: (1) на основе модели сети и вероятных нарушителей формируется граф атак; (2) в реальной сети формируется сеть связанных сенсоров, которые позволяют обнаруживать отдельные атакующие действия; система мониторинга позволяет построить общую картину событий, происходящих в сети, на основе собранной от сенсоров информации; (3) далее общая система управления ищет соответствия между графами атак и событиями в реальной сети. Таким образом, на основе анализа инцидентов с учетом деревьев атак становится возможным делать выводы о том, что существует большая вероятность того, что инциденту «производится сканирование хоста С хостом В» предшествовал необнаруженный инцидент «хост В был атакован хостом А» и что последующим действием нарушителя будет «хост С подвергается атаке со стороны хоста В».

2. Уточнены и доработаны формальные модели и программные прототипы компонентов анализа защищенности компьютерных систем и сетей и определения рисков безопасности информации.

Предлагаемый подход к анализу защищенности и определению рисков безопасности основывается на иерархической системе показателей защищенности, специфицирующей различные уровни представления компьютерной системы, и включает показатели, основанные на современных исследованиях в области анализа защищенности.
Разработанная система показателей защищенности включает следующие уровни: топологический уровень, уровень графа атак, уровень атакующего, уровень событий и уровень интегральных показателей. Каждый уровень включает три категории показателей: основные, стоимостные показатели и показатели 0-дня.
Взаимосвязи между уровнями определяют порядок вычисления показателей в рамках разработанного подхода и информацию, учитываемую в процессе их вычисления.
Первые три уровня относятся к статическому режиму работы системы. На топологическом уровне на основе модели системы и информации об уязвимостях и слабых местах системы рассчитываются следующие основные показатели: Уязвимость хоста, Слабость хоста, Внутренняя

критичность, Внешняя критичность, Процент систем без известных критичных уязвимостей; следующие показатели 0-дня: Уязвимость хоста к атакам нулевого дня; и следующие стоимостные показатели: Ценность хоста для бизнеса. При расчете показателей используются как известные, так и модифицированные методики.
На уровне графа атак на основе графа атак, с учетом информации с предыдущего топологического уровня, рассчитываются следующие основные показатели: Критичность атакующих действий, Потенциал атаки, Ущерб от атаки; следующие показатели 0-дня: Потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Стоимостной ущерб от атаки, Затраты на реагирование.
На уровне атакующего на основе профиля атакующего, с учетом информации с двух предыдущих уровней, рассчитываются следующие основные показатели: Уровень навыков атакующего, Профильный потенциал атаки; следующие показатели 0-дня: Профильный потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Профильный стоимостной ущерб от атаки, Профильные затраты на реагирование. Профиль атакующего при этом включает уровень навыков атакующего и его потенциальные цели, и может корректироваться в соответствии с информацией, полученной со следующего уровня событий.
Уровень событий относится к динамическому режиму работы системы и позволяет корректировать оценки показателей в соответствии с получаемыми событиями и тем самым отслеживать появление и развитие атаки в системе, определять профиль атакующего и прогнозировать его дальнейшие действия. На уровне событий рассчитываются следующие основные показатели: Позиция атакующего, Динамический уровень навыков атакующего, Вероятностный уровень навыков атакующего, Динамический потенциал атаки; следующие показатели 0-дня: Динамический потенциал атаки с учетом нулевого дня; и следующие стоимостные показатели: Динамический стоимостной ущерб от атаки, Динамические затраты на реагирование.
Интегральные показатели могут рассчитываться на основе показателей любого уровня на основе различных методик, что позволяет иметь оценки разной степени точности на разных уровнях работы системы. При этом сложность алгоритмов увеличивается с ростом количества учитываемой информации. На интегральном уровне рассчитываются следующие основные показатели: Уровень риска, Уровень защищенности, Поверхность атаки.

3. Уточнены и доработаны формальные модели и программные прототипы компонентов верификации политики безопасности.
формальные модели и программные прототипы компонентов верификации политики безопасности были доработаны для решения задачи проверки сетевых информационных потоков на наличие аномалий политик безопасности. Например, один из типов аномалий, на выявление которых направлена верификация, связан с аномалией «затемнения». Наличие данной аномалии предполагает, что некоторое правило никогда не срабатывает из-за того, что имеется одно или несколько правил с более высокими приоритетами, его «перекрывающих». Аномалия свидетельствует о вероятной ошибке в политике, которую необходимо пересмотреть.
Сетевые информационные потоки и правила политики специфицированы на основе следующих кортежей:
InformationFlow = < host1, host2, user1, user2, interface1, interface2, type >,
FilteringRule = < host1, host2, user1, user2, interface1, interface2, type, action >,
где host1, host2 – хосты отправителя и получателя соответственно; user1, user2 – пользователь-отправитель и пользователь-получатель; interface1, interface2 – виды аппаратных интерфейсов отправителя и получателя; type – тип информационного потока.
Под типом информационного потока понимается разновидность данных, которые он инкапсулирует. Типы потоков различаются, как в соответствии с разновидностью передаваемой информации (например, пользовательские данные, критически важные данные, контрольные суммы, ключи шифрования, сертификат защиты и др.), так и в соответствии с формой, в которой информация представлена (например, нешифрованное и шифрованное сообщения, сжатое сообщение).
Сущность метода «проверки на модели», применяемого для обнаружения аномалий, заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов компонента, принимающего решения о разрешении или отклонении таких запросов на основе политик.

Последовательность действий при переборе зависит от условий, которые сформулированы на языке линейной темпоральной логики и выражают корректные состояния системы. Состояние системы определяется набором значений переменных, а изменение состояния вызывается выполняющимися в ней параллельными процессами.
Процесс, который должен выполняться в очередной момент времени, выбирается случайно. Система рассматривает все возможные последовательности шагов для заданных процессов и сигнализирует о потенциальном некорректном состоянии. После этого пользователю выдается «трасса», т.е. последовательность шагов, ведущая к некорректному состоянию системы относительно заданных условий.
Основными входными данными верификации сетевых информационных потоков являются описания правил политики контроля сетевых информационных потоков и структура сети, содержащей встроенные устройства, на языке описания системы, а также выявляемые виды аномалий.
На первом этапе верификации входные данные преобразуются во внутренний формат системы верификации. Затем, на втором этапе, строится общая модель системы для верификации правил разрешения/запрета информационных потоков, представленная в виде конечного автомата и инициализированная входными данными во внутреннем формате. Аномалии в модели выражены формальными утверждениями. В рамках метода «проверки на модели» эти формальные утверждения будут являться свойствами корректности, нарушение которых приводит исследуемую систему в некорректное состояние. На третьем этапе общая модель для верификации правил разрешения/запрета информационных потоков верифицируется специальными программными средствами, реализующими метод «проверки на модели». В процессе верификации выявляются все некорректные состояния системы. На завершающем этапе полученные результаты верификации интерпретируются. Если были обнаружены аномалии, то создается описание, содержащее ситуацию и информационный поток, приводящий к возникновению аномалии, а также тип аномалии.
Преимущество предложенного подхода к верификации информационных потоков – возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам можно отнести большой объем необходимых вычислительных ресурсов для анализа сложных моделей; «ложные срабатывания», то есть предупреждения об аномалиях, которых в реальной системе не будет; и неполнота, так как проверяется не реальная система, а ее модель.

4. Уточнены и доработаны формальные модели и программные прототипы компонентов активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения.
На текущем этапе основное внимание было уделено аспекту построения системы детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных с учетом установленных требований - устойчивости к ошибкам, инкрементальности и оперативности процедур обучения и валидации системы детектирования. Выполнение требования устойчивости к ошибкам достигается за счет выбраковки всех неоднозначных правил классификации, выведенных на каждой итерации обучения для каждого используемого набора признаков. Соблюдение требования инкрементальности обучения обеспечивается за счет выделения каждой конечной модели принятия решения в отдельный классификатор, включающийся в общую комбинированную схему принятия решения. Требование оперативности обучения обеспечивается как за счет введения процедур приоритезации отдельных групп признаков в соответствии со степенью их значимости, так и за счет использования методов комбинирования классификаторов. Предложена модель инкрементального обновления знаний об угрозах, следующая принципу периодического поступления на вход системы новых наборов заранее исследованных объектов, имеющих установленный класс вредоносности. В качестве основных групп признаков использовались как поведенческие, так и структурные особенности анализируемых объектов. В качестве базового метода классификации применялись деревья решений (далее Decision Trees, DT), основные методы метаклассификации - голосование (Voting), бустинг (Boosting) и стэкинг (Stacking). Комбинирование классификаторов производилось на основе совмещения отдельных групп признаков в рамках отдельных моделей принятия решения. Показана применимость предложенных моделей и методик детектирования потенциально вредоносных исполняемых программных модулей на основе статических позиционно-зависимых

данных на примере анализа исполняемых файлов формата Portable Executable (PE32). Общие положения подхода могут быть использованы для других носителей угроз, в том числе и комбинированных. Процесс извлечения признаков основан на использовании программного средства разбора файлов данного формата (парсера). Данное программное средство способно идентифицировать программную точку входа анализируемого объекта, непрерывный физический участок (секцию) объекта, включающий точку входа и обеспечивать операцию чтения идентифицированной секции по допустимому региону относительных виртуальных адресов.

5. Осуществлена реализация и теоретическая и экспериментальная оценка предложенных моделей и методов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур.
Реализован комплекс программных компонентов, которые предназначены для мониторинга и управления информационной безопасностью в компьютерных сетях и системах, в том числе были получены следующие свидетельства о государственной регистрации программ для ЭВМ:
- Котенко И.В., Дойникова Е.В., Чечулин А.А. Вычисление показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности. Свидетельство № 2014661026. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
- Котенко И.В., Чечулин А.А. Формирование модели нарушителя для анализа защищенности информационно-телекоммуникационных систем. Свидетельство № 2014661028. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
- Десницкий В.А., Котенко И.В. Верификация сетевых информационных потоков для защиты информационно-телекоммуникационных систем со встроенными устройствами. Свидетельство № 2014661027. Зарегистрировано в Реестре программ для ЭВМ 22.10.2014.
- Саенко И.Б., Агеев С.А., Чечулин А.А. Поддержка принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи. Свидетельство № 2014660775. Зарегистрировано в Реестре программ для ЭВМ 15.10.2014.
- Саенко И.Б., Скорик Ф.А., Чечулин А.А. Решение задачи оценки и прогнозирования состояния распределенных информационных систем. Свидетельство № 2014660856. Зарегистрировано в Реестре программ для ЭВМ 17.10.2014.

Теоретическая и экспериментальная оценка предложенных моделей и методов моделирования атак, анализа защищенности и определения рисков, базировалась на реализации следующих этапов работы с прототипами компонентов моделирования атак, анализа защищенности и определения рисков: формирование модели сети (эксперименты проводились для сетей различного объема и различной структуры зависимостей сервисов); задание параметров (моделей атакующего, критичностей, и т.п.); формирование графа атак; анализ графа атак; обработка событий безопасности и тревог. Модели атакующего определялись позицией атакующего в системе (внешний или внутренний), уровнем знаний атакующего и его целями в системе. События безопасности определялись соответствующим хостом системы и уровнем ущерба на хосте. Для смоделированных атак и выбранных моделей атакующих вычислялись показатели защищенности разных уровней. Результаты экспериментов показали достаточно высокую степень совпадения между заданными путями атаки и профилями атакующих, определенными на основе вычисления показателей. Тем не менее, проблемой являются достаточно высокие временные затраты на уровне событий, что неприемлемо для режима работы во времени, близком к реальному. Решение этой проблемы предполагается осуществить на следующем этапе исследований.

Разработанные программные прототипы компонентов верификации политики безопасности включают средства для верификации сетевых информационных потоков. Предложенная методика в части верификации сетевых информационных потоков была использована при анализе защищенности системы автоматизированного контроля расхода электроэнергии потребителями. Вследствие технических упрощений ограничением осуществленной реализации является задание параметров правил политики лишь при помощи либо определенных значений правил (конкретных хостов, интерфейсов, пользователей), либо с использованием специальных идентификаторов any, обозначающих все возможные значения данного параметра. В общем случае предполагается задание заранее нефиксированных множеств параметров и любых их подмножеств (в частности использование конструкций типа «все значения кроме x1, x2, x3»). Правила политики были

сформированы, исходя из имеющихся спецификаций системы автоматизированного контроля расхода электроэнергии потребителями.
Были проведены эксперименты по внесению в политику экземпляров аномалий «затенения», имитирующих потенциальные ошибки в процессе ее разработки. Выполнение методики позволило выявить каждую из внесенных аномалий. На основе результатов методики первоначальная политика корректировалась, после чего методика применялась снова, и новая политика была признана свободной от аномалий «затенения». Проведенные эксперименты по моделированию систем с большим количеством вовлеченных объектов, ролей, типов данных и правил разрешения/запрета подтверждают эффективность предложенной методики для систем индустриального уровня. Так как типовые конфликты и аномалии выявляются по большей части эвристически, сложно говорить о каких-либо универсальных способах их разрешения. Устранение конфликта/аномалии определяется, в первую очередь, его/ее контекстом, включающим специфичные требования и допущения защиты, риски информационной безопасности, режимы работы, вовлеченные компоненты защиты, используемые интерфейсы и т.п.
Отметим, что для верификации политики безопасности в части контроля сетевых информационных потоков недостаточно использовать только парные сравнения правил политики, а нужен именно анализ срабатываний правил политики «в динамике», то есть с использованием моделирования на основе «проверки на модели».

Прототипы компонентов активного аудита были реализованы в среде Rapid Miner 5.2 с целью анализа исполняемых файлов на предмет наличия вредоносного программного обеспечения на базе статической позиционно-зависимой модели объектов формата PE32. Практические работы по проверке методики обнаружения, основанной на статической позиционно-зависимой модели представления, показали, что показатель точности обнаружения AUC (площадь ROC-кривой) достигает значения 0.98 при использовании классификатора, обученного на пространстве из 250 признаков. Результаты сравнимы с результатами оценивания существующих быстрых статических методик обнаружения вредоносного программного обеспечения, основанных на использовании n-грамм и простых подходах анализа кода (дизассемблирования). Показатели точности могут быть улучшены при дальнейшем расширении пространства признаков. С точки зрения характеристик времени обучения (принятия решения) и ресурсопотребления данный подход выгодно отличается в лучшую сторону за счет ограничения потенциально возможного количества признаков, определяемым комбинацией значения и его смещения.

3.7 Степень новизны полученных результатов

Основные научные результаты являются новыми и оригинальными, они основываются на разработках исполнителей проекта, выполненных ранее и выполняемых в настоящее время, а также базируются на современных достижениях в области защиты информации, интеллектуального анализа данных, онтологического моделирования, разработки и применения механизмов логического вывода и др.

3.8 Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения 2014 года проекта, соответствуют мировому уровню. Авторы проекта опубликовали полученные результаты в нескольких журналах, сборниках и трудах конференций, а также апробировали результаты на множестве различных российских и международных конференций, в частности, на 22-й Европейской международной конференции по параллельной, распределенной и сетевой обработке информации (PDP 2014, Турин, 12-14 февраля 2014 г.), 16-й международной конференции «РусКрипто 2014» по криптологии, стеганографии, цифровой подписи и системам защиты информации (Московская область, г.Солнечногорск, 25-28 марта 2014 г.), IV международной научно-практической конференции «ИнтеллектТранс-2014» (Санкт-Петербург, 3 и 4 апреля 2014 г.), Азиатской конференции по доступности, надежности и безопасности (AsiaARES 2014, Бали, Индонезия, 14-17 апреля 2014 г.), XVII-й Всероссийской научно-практической конференции "Актуальные проблемы защиты и безопасности" (Санкт-Петербург, 1 - 4 апреля 2014 г.), Международном форуме по практической безопасности Positive Hack Days (Москва, 21-22 мая 2014 г.), Международной научно-практической конференции "Теоретические и прикладные проблемы информационной безопасности" (19 июня 2014 года, г. Минск, Беларусь, 2014 г.), 23-й Общероссийской научно-технической конференции «Методы и технические средства обеспечения

безопасности информации» (Санкт-Петербург, 30 июня - 3 июля 2014 г.), 14-й международной индустриальной конференции по Data Mining (ICDM 2014, Санкт-Петербург, 16-21 июля 2014 г.), 6-м IEEE Международном симпозиуме по безопасности киберпространства (CSS 2014, Париж, Франция, 20-22 августа 2014 г.), 8-м Международном симпозиуме по интеллектуальным распределенным вычислениям (IDC'2014, Мадрид, Испания, 3-5 сентября 2014 г.), Международной конференции по доступности, надежности и безопасности (ARES-2014, Фрибур, Швейцария, 8-12 сентября 2014 г.), Международном Конгрессе по интеллектуальным системам и информационным технологиям («IS&IT'14», Дивноморское, 2-8 сентября, 2014 г.), Четырнадцатой национальной конференции по искусственному интеллекту с международным участием (КИИ-2014, г. Казань, 24–27 сентября 2014 г.) и др.

3.9 Методы и подходы, использованные в ходе выполнения проекта (описать, уделив особое внимание степени оригинальности и новизны)

(1) механизмы обеспечения информационной безопасности в компьютерных сетях (в том числе новые технологии разграничения доступа и обнаружения вторжений);
(2) методы системного анализа и теории систем в части их применения для разработки общей архитектуры и архитектуры отдельных компонентов системы интеллектуальных сервисов защиты информационных и сетевых ресурсов в современных и перспективных компьютерных системах;
(3) методы агентно-ориентированного моделирования, генерации трафика на основе моделей, эмуляции и виртуализации сетевых процессов, имитационного моделирования на уровне сетевых пакетов; (4) методы визуального анализа информации; (5) методы объединения (слияния) данных и информации; (6) методы реализации логического вывода на основе исчисления событий и «проверки на модели» (model checking) в части их применения к управлению уровнями защищенности современных компьютерных систем и сетей; (7) методы нечетких когнитивных карт и нечеткого логического вывода, дополняющих положения теории математического программирования, массового обслуживания, случайных процессов и графов; (8) онтологический подход к моделированию предметной области систем защиты информации в части создания и применении онтологии, охватывающей метрики защищенности, структурные элементы информационно-телекоммуникационной системы и контрмеры по обеспечению требуемого уровня защищенности; (9) методы вывода, основанные на знаниях о выполняемых действиях и предсказании намерений и планов оппонента, а также рефлексивные процессы и модели антагонистических процессов; (10) методы оценки защищенности и анализа рисков; (11) методы интеллектуального анализа данных, в том числе на базе статической и динамической информации, комбинирования классификаторов, обучения и классификации на зашумленных наборах данных; и др.

3.10.1.1 Количество научных работ по Проекту, опубликованных в 2014 году (цифрами)

93

3.10.1.2 Из них в изданиях, включенных в перечень ВАК

15

3.10.1.3 Из них в изданиях, включенных в системы цитирования (Web of Science, Scopus, Web of Knowledge, Astrophysics, PubMed, Mathematics, Chemical Abstracts, Springer, Agris, GeoRef)

16

3.10.2 Количество научных работ, подготовленных в ходе выполнения Проекта и принятых к печати в 2014 году (цифрами)

3

3.11 Участие в 2014 году в научных мероприятиях по тематике Проекта (указать названия мероприятий)

- 22-я Европейская (Euromicro) международная конференция по параллельной, распределенной и сетевой обработке информации (PDP 2014), Турин, 12-14 февраля 2014 г. (И.В.Котенко).
- 16-я международная конференции «РусКрипто 2014» по криптологии, стеганографии, цифровой подписи и системам защиты информации, Московская область, г.Солнечногорск, 25-28 марта

2014 г. (И.В.Котенко, В.А.Десницкий, А.А.Чечулин, Федорченко А.В.).
- IV международная научно-практическая конференция «ИнтеллектТранс-2014». Санкт-Петербург. 3 и 4 апреля 2014 г. (И.В.Котенко, И.Б.Саенко).
- Азиатская конференция по доступности, надежности и безопасности (AsiaARES 2014). Бали, Индонезия, 14-17 апреля 2014 г. (И.В.Котенко).
- Всероссийская научно-практическая конференция "Актуальные проблемы защиты и безопасности". Санкт-Петербург, 1 - 4 апреля 2014 г. (И.В.Котенко).
- Международный форум по практической безопасности Positive Hack Days. Москва, 21-22 мая 2014 г. (И.В.Котенко, В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин, А.В.Федорченко).
- Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Беларусь, 2014 г. (И.Б.Саенко).
- 23-я Общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, 30 июня - 3 июля 2014 г. (И.Б.Саенко).
- 14-я индустриальная конференция по Data Mining (ICDM 2014), Санкт-Петербург, 16-21 июля 2014 г. (И.В.Котенко).
- 6-й IEEE Международный симпозиум по безопасности киберпространства (CSS 2014). Париж, Франция. 20-22 августа 2014 г. (И.В.Котенко).
- 8-й Международный симпозиум по интеллектуальным распределенным вычислениям (IDC'2014). Мадрид, Испания. 3-5 сентября 2014 г. (И.В.Котенко).
- Международная конференция по доступности, надежности и безопасности (ARES-2014), Фрибур, Швейцария, 8-12 сентября 2014 г. (И.В.Котенко).
- Международный Конгресс по интеллектуальным системам и информационным технологиям «IS&IT’14», Дивноморское, 2-8 сентября, 2014 г. (И.Б.Саенко).
- Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014, г. Казань, 24–27 сентября 2014 г. (И.Б.Саенко).
- Конференция "Информационные технологии в управлении" (ИТУ-2014). Санкт-Петербург, 7-9 октября 2014 г. (И.В.Котенко, И.Б.Саенко, В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин, А.В.Федорченко).
-XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Санкт-Петербург, 23-25 октября 2014 г. (И.В.Котенко, И.Б.Саенко, В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин, А.В.Федорченко).
- Конференция Zero Nigts 2014. Москва, 13-14 ноября 2014 г. (В.А.Десницкий, Е.В.Дойникова, А.А.Чечулин, А.В.Федорченко).
- 6-я Научно-практическая конференция "Информационная безопасность. Невский диалог 2014", Санкт-Петербург, 12-13 ноября 2014 г. (А.А.Чечулин, А.В.Федорченко).
- Научно-практическая конференция "Реализация прикладных научных исследований и экспериментальных разработок по приоритетному направлению Информационно - телекоммуникационные системы в 2014 году в рамках федеральной целевой программы "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014 – 2020 годы". Москва, Зеленоград, 2-3 декабря 2014 г. (И.В.Котенко, И.Б.Саенко).
- Научно-техническая конференция «Инновации Северо-Запада». Санкт-Петербург, 15-16 декабря 2014 г. (И.Б.Саенко, В.А.Десницкий, А.А.Чечулин).

3.12 Участие в 2014 году в экспедициях по тематике Проекта, которые проводились при финансовой поддержке Фонда (указать номера Проектов)

не заполнено

3.13 Финансовые средства, полученные в 2014 году от РФФИ (указать общий объем, в руб.)

520000,00

3.14 Адреса (полностью) ресурсов в Интернете, подготовленных авторами по данному проекту, например, http://www.somewhere.ru/mypub.html

http://comsec.spb.ru/ru/staff/kotenko http://comsec.spb.ru/en/staff/kotenko
http://comsec.spb.ru/ru/projects/ http://comsec.spb.ru/en/projects

3.15 Библиографический список всех публикаций по Проекту, опубликованных в 2014 году, в порядке

значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

1. Igor Kotenko, Andrey Shorov, Andrey Chechulin, Evgenia Novikova. Dynamical Attack Simulation for Security Information and Event Management // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems, Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.219-234. (Scopus).
2. Igor Kotenko, Olga Polubelova, Igor Saenko. Logical Inference Framework for Security Management in Geographical Information Systems // V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems, Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14, Springer-Verlag, Berlin, Heidelberg, 2014. P.203-218. (Scopus).
3. Igor Kotenko, Elena Doynikova, Andrey Chechulin. Security metrics based on attack graphs for the Olympic Games scenario // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.561-568. (WoS, Scopus).
4. Philipp Nesteruk, Lesya Nesteruk, Igor Kotenko. Creation of a Fuzzy Knowledge Base for Adaptive Security Systems // Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.574-577. (WoS, Scopus).
5. Igor Kotenko, Elena Doynikova. Security Assessment of Computer Networks based on Attack Graphs and Security Events // The 2014 Asian Conference on Availability, Reliability and Security (AsiaARES 2014). In conjunction with ICT-EurAsia 2014. Bali, Indonesia, April 14th – 17th, 2014. / Linawati et al. (Eds.): ICT-EurAsia 2014, Lecture Notes in Computer Science (LNCS), Vol.8407. IFIP International Federation for Information Processing (2014). Springer. 2014, P.462-471. (WoS, Scopus).
6. Igor Kotenko, Andrey Chechulin, Andrey Shorov, Dmitry Komashinsky. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. P. Perner (Ed.): 14th Industrial Conference on Data Mining (ICDM 2014), July 16 – 21, 2014, St. Petersburg, Russia. Lecture Notes in Artificial Intelligence (LNAI), DOI 10.1007/978-3-319-08976-8. P. 39–54. ISSN 0302-9743, ISBN 978-3-319-08975-1. (WoS, Scopus).
7. Kotenko I., Shorov A. Simulation of bio-inspired security mechanisms against network infrastructure attacks // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.127-133. (WoS, Scopus).
8. Igor Kotenko, Igor Saenko. Design of Virtual Computer Networks: Data Mining by Genetic Algorithms // Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Springer-Verlag, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain. Springer-Verlag. P.95-105. (WoS, Scopus).
9. Igor Kotenko, Elena Doynikova. Security Evaluation Models for Cyber Situational Awareness // The 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France. 2014. Los Alamitos, California. IEEE Computer Society. 2014. P.1229-1236. (WoS, Scopus).
10. Igor Kotenko, Evgenia Novikova. Visualization of Security Metrics for Cyber Situation Awareness // The 1st International Software Assurance Workshop (SAW 2014). In conjunction with the 9th International Conference on Availability, Reliability and Security (ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. IEEE Computer Society. 2014. P.506-513. (WoS, Scopus).
11. Evgenia Novikova, Igor Kotenko. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014, P.63-78. (WoS, Scopus).
12. Vasily Desnitsky, Igor Kotenko. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // 4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), Vol.8708. Springer-Verlag. 2014. P.194-210. (WoS, Scopus).
13. Igor Kotenko, Elena Doynikova. Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.5, No.3, September 2014. P.14-29. (Scopus)
14. Igor Saenko, Igor Kotenko. Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and

Dependable Applications (JoWUA), Vol.5, No.4, December 2014. (Scopus)
15. Andrey Shorov, Igor Kotenko. The Framework for Simulation of Bio-inspired Security Mechanisms Against Network Infrastructure Attacks // The Scientific World Journal, Volume 2014 (2014), Article ID 172583, 11 pages. http://dx.doi.org/10.1155/2014/172583. (WoS, IF=1.730, Scopus).
16. I.V. Kotenko and I. B. Saenko. Creating New Generation Cybersecurity Monitoring and Management Systems // Herald of the Russian Academy of Sciences, 2014, Vol.84, No.6. P.993–1001. ISSN 1019-3316. DOI: 10.1134/S1019331614060033 (Scopus IF=0.170, WoS).
17. Котенко И.В., Саенко И.Б. Предложения по онтологическому представлению и гибридному хранению данных о событиях безопасности в АСУ железнодорожного транспорта // Технические науки — от теории к практике, № 29, 2014. Новосибирск: Изд. «СибАК», 2014. С.28-32.
18. Котенко И.В., Саенко И.Б. Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта // Естественные и математические науки в современном мире. 2014. № 14. Новосибирск: Изд. «СибАК», С. 46-50.
19. Котенко И.В., Саенко И.Б. Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта // Технические науки - от теории к практике. Новосибирск: Изд. «СибАК», 2014. № 30. С. 18-22.
20. Котенко И.В., Саенко И.Б., Чечулин А.А. Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах // Вопросы радиоэлектроники. Сер. СОИУ. 2014. Вып. 1. С. 170–180.
21. Чечулин А.А., Котенко И.В. Построение графов атак для анализа событий безопасности // Безопасность информационных технологий, № 3, 2014, С.135-141.
22. Котенко И.В., Дойникова Е.В. Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов // Проблемы информационной безопасности. Компьютерные системы, № 2, 2014. С.19-36.
23. Десницкий В.А., Котенко И.В. Проектирование и верификация защищенных систем со встроенными устройствами на основе экспертных знаний // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.16-22.
24. Чечулин А.А., Котенко И.В. Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.56-59.
25. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Проблемы информационной безопасности. Компьютерные системы, № 3, 2014. С.131-135.
26. Котенко И.В., Саенко И.Б. К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001.
27. Котенко И.В., Саенко И.Б., Юсупов Р.М. Новое поколение систем мониторинга и управления инцидентами безопасности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. СПбГПУ, 2014, № 3 (198), С.7-18.
28. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы данных уязвимостей // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.62-67. ISSN 0021-3454.
29. Дойникова Е.В., Котенко И.В. Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности // Изв. вузов. Приборостроение, Т.57, № 10, 2014, С.72-77. ISSN 0021-3454.
30. Десницкий В.А., Котенко И.В. Использование экспертных знаний для разработки защищенных систем со встроенными устройствами // Информационные технологии и вычислительные системы, № 4, 2014, С.17-32.
31. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей // Информационно-управляющие системы, 2014, №5, С.72-79.
32. Котенко И.В., Саенко И.Б. О задачах обеспечения кибербезопасности в инфраструктурах "электронного города" на основе методов искусственного интеллекта // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.618-622. ISBN 978-5-91995-042-4.
33. Чечулин А.А., Котенко И.В. Разработка системы защиты пользователей от нежелательной информации в сети Интернет // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.642-647. ISBN 978-5-91995-042-4.

34. Котенко И.В., Чечулин А.А. Применение технологии обработки больших данных для защиты сетевой инфраструктуры // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.614-617. ISBN 978-5-91995-042-4.
35. Федорченко А. В., Чечулин А.А., Котенко И.В. Интегрированная база данных уязвимостей в системе оценки защищенности компьютерных сетей // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.638-641. ISBN 978-5-91995-042-4.
36. Десницкий В.А. Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.596-600. ISBN 978-5-91995-042-4.
37. Дойникова Е.В. Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.601-604. ISBN 978-5-91995-042-4.
38. Саенко И.Б., Куваев В.О. О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.631-637. ISBN 978-5-91995-042-4.
39. Агеев С.А., Саенко И.Б. Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов // Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2014. С.556-562. ISBN 978-5-91995-042-4.
40. Десницкий В.А. Концептуальная комбинированная модель системы защиты встроенных устройств // Журнал "Инновации в науке". Изд. НП "СибАК", №38, 2014, С.55-59. ISSN: 2308-6009.
41. Десницкий В.А. Разработка модели знаний для проектирования защищенных встроенных устройств // Журнал "Естественные и математические науки в современном мире". Изд. НП "СибАК", №23, 2014, С.35-40.
42. Десницкий В.А., Чечулин А.А. Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами // Журнал «Технические науки — от теории к практике». Изд. НП "СибАК", №38, 2014, С.7-21.
43. 90. Котенко И.В., Саенко И.В., Чечулин А.А. Проактивное управление информацией и событиями безопасности в сетях NGN // Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты», Санкт-Петербург, СПб ГУТ им Бонч-Бруевича. 23–25 июня 2014 года.
44. Носков А.Н., Чечулин А.А., Тарасова Д.А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. Вып.6 (37). СПб.: Наука, 2014.
45. Агеев С.А., Саенко И.Б., Егоров Ю.П., Гладких А.А., Богданов А.В. Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. Вып. №3 (37), 2014. ISSN 1991-2927. С.78-88.
46. Куваев В.О., Саенко И.Б. Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве // Проблемы экономики и управления в торговле и промышленности, № 7 (007), 2014. – С. 101-104. ISSN 2309-3064.
47. Саенко И.Б., Куваев В.О., Алышев С.В. Подход к построению системы показателей качества единого информационного пространства // Естественные и математические науки в современном мире, 2014. № 14. С. 51-56.
48. Igor Kotenko, Andrey Chechulin. Fast Network Attack Modeling and Security Evaluation based on Attack Graphs // Journal of Cyber Security and Mobility, Vol.3, No.1, P.27–46.
49. Котенко И.В., Новикова Е.С. Модели и методики визуального анализа данных для решения задач компьютерной безопасности // Шестнадцатая Международная конференция

“РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
50. Чечулин А.А., Котенко И.В.Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
51. Десницкий В.А.Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
52. Федорченко А.В., Чечулин А.А., Котенко И.В.Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Шестнадцатая Международная конференция “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г. http://www.ruscrypto.ru/
53. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта // Интеллектуальные системы на транспорте: тезисы докладов IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: Петербургский гос. ун-т путей сообщения, 2014. С.21.
54. Котенко И.В., Саенко И.Б. О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта // Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014». – СПб.: ПГУПС, 2014. С.196-203.
55. Котенко И.В., Юсупов Р.М. Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах // XVII-я Всероссийская научно-практическая конференция "Актуальные проблемы защиты и безопасности". Санкт-Петербург, 1 - 4 апреля 2014 г.
56. Котенко И.В., Новикова Е.С. Визуальная аналитика на страже информационной безопасности // Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru
57. Саенко И.Б., Котенко И.В. Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
58. Федорченко А.В., Чечулин А.А., Котенко И.В. Интегрированная база данных уязвимостей // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
59. Чечулин А.А. Анализ и классификация возможных изменений, происходящих в компьютерной сети и их влияние на деревья атак // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь,. 2014.
60. Нестерук Ф. Г. Специфика двухуровневой организации адаптивных систем защиты информации // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
61. Дойникова Е.В. Вычисление показателей защищенности в системах мониторинга и управления безопасностью // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
62. Десницкий В.А., Дойникова Е.В. Разработка компонентов защиты встроенных устройств с учетом экспертных знаний // Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь, 2014.
63. Котенко И.В., Саенко И.Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном

транспорте // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.97-98.
64. Котенко И.В., Чечулин А.А., Десницкий В.А. Особенности построения системы защиты информации в кибер-физических системах // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.67-69.
65. Десницкий В.А., Котенко И.В. Конфигурирование информационных систем со встроенными устройствами для обеспечения комплексной безопасности железнодорожного транспорта // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.89-90.
66. Десницкий В.А., Котенко И.В. Комбинированная модель защиты информационно-телекоммуникационных систем концепции «Интернет вещей» // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.65-66.
67. Десницкий В.А., Чечулин А.А. Верификация информационно-телекоммуникационных систем со встроенными устройствами на основе обобщенной модели нарушителя // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.66-67.
68. Федорченко А.В. Анализ уязвимостей по временным характеристикам на основе открытой базы данных X-Force // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.104-105.
69. Дойникова Е.В. Подход к оцениванию защищенности на основе графов атак в системах управления информацией и событиями безопасности // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.90-91.
70. Агеев С.А., Саенко И.Б. Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.59-60.
71. Куваев В.О., Саенко И.Б. Подход к решению задачи разграничения доступа в разнородном информационном пространстве // Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 года. Санкт-Петербург. Издательство Политехнического университета. 2014. С.33-34.
72. Котенко И.В., Саенко И.Б. Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.2. С.271-276. 978-5-9221-1572-8.
73. Саенко И.Б., Котенко И.В. Подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14». Научное издание в 4-х томах. М.: Физматлит, 2014. Т.1. С.35-40. ISBN 978-5-9221-1572-8.
74. Котенко И.В., Саенко И.Б. Интеллектуальная система мониторинга и управления инцидентами кибербезопасности // Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции. Т.3. Казань: Изд-во РИЦ «Школа», 2014. С.219-227.
75. Дойникова Е.В., Котенко И.В. Анализ и применение показателей защищенности в SIEM-системах на основе графов атак и зависимостей сервисов // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). Труды конференции. СПб.: СПОИСУ, 2014.
76. Новожилов Д.А., Чечулин А.А. Методы определения основного языка веб-страниц // XIV Санкт-Петербургская Международная Конференция "Региональная информатика-2014" ("РИ-

2014”). Материалы конференции. СПб., 2014. С.155-156.
77. Чечулин А.А., Комашинский Д.В. Решение задачи классификации сайтов на иностранных языках в сети Интернет // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.169-170.
78. Чечулин А.А., Котенко И.В. Программный прототип компонента аналитического моделирования атак для систем управления информацией и событиями безопасности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.170-171.
79. Десницкий В.А. Анализ перспективных систем со встроенными устройствами для формирования экспертных знаний в области проектирования защищенных информационно-телекоммуникационных систем // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.130.
80. Десницкий В.А., Котенко И.В. Концептуальная комбинированная модель системы защиты встроенных устройств и ее применение для конфигурирования компонентов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.131.
81. Дойникова Е.В., Котенко И.В. Оценивание защищенности в автоматизированных системах управления РЖД // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.132-133.
82. Дойникова Е.В. Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.132.
83. Федорченко А.В. Методы интеграции баз уязвимостей для улучшения анализа защищенности компьютерных систем // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.165-166.
84. Федорченко А.В. Обзор механизмов корреляции событий безопасности в SIEM-системах // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.166.
85. Агеев С.А., Саенко И.Б. Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.116-117.
86. Котенко И.В., Саенко И.Б. Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.144.
87. Котенко И.В., Саенко И.Б. Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.143.
88. Левшун Д.С., Чечулин А.А. Построение классификационной схемы существующих методов корреляции событий безопасности // XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014. С.148-149.
89. Брюханов А.В., Архипов Ю.А., Лепнев П.А., Чечулин А.А., Котенко И.В. Решение задачи формирования списков информационных объектов и их связей для визуализации данных при мониторинге и управлении информационной безопасностью // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.65-69.
90. Чечулин А.А., Котенко И.В., Дойникова Е.В. Методика анализа истории событий безопасности, прогнозирования действий нарушителя и их последствий // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.69-72.
91. Бушуев С.Н., Копчак Я.М., Ногин С.Б., Десницкий В.А. Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей

// Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.73-77.
92. Безродный И.В., Смирнов Д.Б., Саенко И.Б., Котенко И.В., Волков А.А. Основы технологии агрегации, нормализации и анализа данных для мониторинга безопасности сетей «Интернет вещей» // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.77-81.
93. Полушин В.Ю., Малоземов Д.Г., Саенко И.Б., Чечулин А.А., Зорохович С.В. Программно-аппаратный стенд генерации наборов тестовых гетерогенных данных для моделирования сети «Интернет вещей» // Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2004. С.81-85.

3.16 Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта

Информационно-телекоммуникационные системы

3.17 Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта

Технологии информационных, управляющих, навигационных систем

3.18 Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты данного проекта

Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения.

Основные результаты проекта

Основные цели проекта на 2014 год были связаны с продолжением работ по разработке, прототипированию, теоретической и экспериментальной оценке моделей и методов мониторинга и управления информационной безопасностью в компьютерных сетях и системах критических инфраструктур, основывающихся на интеллектуальных сервисах защиты информации, в частности, гибридного многоагентного моделирования компьютерных атак и процессов защиты от них, анализа защищенности компьютерных систем и сетей, анализа рисков безопасности информации, верификации политики безопасности, активного аудита компьютерных систем и сетей и защиты информационных и программных ресурсов от вредоносного программного обеспечения.

В ходе второго этапа проекта 13-01-00843 выполнено уточнение и проведена доработка формальных моделей и программных прототипов компонентов исследовательского моделирования компьютерных атак и процессов защиты от них, анализа защищенности и определения рисков безопасности информации, верификации политики безопасности, активного аудита и защиты информационных и программных ресурсов от вредоносного программного обеспечения. Выполнена теоретическая и экспериментальная оценка предложенных решений. Получены свидетельства о государственной регистрации программ для ЭВМ для вычисления показателей защищенности для анализа текущего состояния информационно-телекоммуникационных систем и поддержки принятия решений по реагированию на инциденты информационной безопасности, формирования модели нарушителя для анализа защищенности информационно-телекоммуникационных систем, верификации сетевых информационных потоков для защиты информационно-телекоммуникационных систем со встроенными устройствами, поддержки принятия решений при оценке рисков угроз информационной безопасности мультисервисных сетей связи, решения задачи оценки и прогнозирования состояния распределенных информационных систем.

Разработанные модели, методики и прототипы программные прототипы компонентов исследовательского моделирования компьютерных атак и процессов защиты от них основаны на построении и анализе графов атак, позволяющих, с одной стороны, оценить защищенность компьютерной сети от атак, а с другой – участвовать в анализе событий безопасности для выявления наиболее вероятных трасс атак и, как следствие, наиболее вероятных нарушителей. Основной особенностью, отличающей предложенные модели и методики от существующих, является способ использования графов атак и учета текущих событий безопасности для идентификации фрагмента графа атак.

Предложенный подход к анализу защищенности и определению рисков безопасности основывается на иерархической системе показателей защищенности, специфицирующей различные уровни представления компьютерной системы, и включает показатели, основанные на современных исследованиях в области анализа защищенности. Разработанная система показателей защищенности включает следующие уровни: топологический уровень, уровень графа атак, уровень атакующего, уровень событий и уровень интегральных показателей. Каждый уровень включает три категории показателей: основные, стоимостные показатели и показатели нулевого дня. Взаимосвязи между уровнями определяют порядок вычисления показателей в рамках разработанного подхода и информацию, учитываемую в процессе их вычисления.

Формальные модели и программные прототипы компонентов верификации политики безопасности были доработаны для решения задачи проверки сетевых информационных потоков на наличие аномалий политик безопасности. Например, один из типов аномалий, на выявление которых направлена верификация, связан с аномалией «затемнения». Наличие данной аномалии предполагает, что некоторое правило никогда не срабатывает из-за того, что имеется одно или несколько правил с более высокими приоритетами, его «перекрывающих». Сущность метода «проверки на модели», применяемого для обнаружения аномалий, заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов компонента, принимающего решения о разрешении или отклонении таких

запросов на основе политик. Преимущество предложенного подхода к верификации информационных потоков – возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам можно отнести большой объем необходимых вычислительных ресурсов для анализа сложных моделей; «ложные срабатывания», то есть предупреждения об аномалиях, которых в реальной системе не будет; и неполнота, так как проверяется не реальная система, а ее модель.

На текущем этапе также решалась задача детектирования вредоносного программного обеспечения на основе методов интеллектуального анализа данных с учетом установленных требований - устойчивости к ошибкам, инкрементальности и оперативности процедур обучения и валидации системы детектирования. Предложена модель инкрементального обновления знаний об угрозах, следующая принципу периодического поступления на вход системы новых наборов заранее исследованных объектов, имеющих установленный класс вредоносности. В качестве основных групп признаков использовались как поведенческие, так и структурные особенности анализируемых объектов. Показана применимость предложенных моделей и методик детектирования потенциально вредоносных исполняемых программных модулей на основе статических позиционно-зависимых данных на примере анализа исполняемых файлов формата Portable Executable (PE32). Общие положения подхода могут быть использованы для других носителей угроз, в том числе и комбинированных.

Теоретическая и экспериментальная оценка предложенных моделей и методов моделирования атак, анализа защищенности и определения рисков, базировалась на реализации следующих этапов работы с прототипами компонентов моделирования атак, анализа защищенности и определения рисков: формирование модели сети (эксперименты проводились для сетей различного объема и различной структуры зависимостей сервисов); задание параметров (моделей атакующего, критичностей, и т.п.); формирование графа атак; анализ графа атак; обработка событий безопасности и тревог.

Разработанные программные прототипы компонентов верификации политики безопасности включают средства для верификации сетевых информационных потоков. Были проведены эксперименты по внесению в политику экземпляров аномалий «затенения», имитирующих потенциальные ошибки в процессе ее разработки. Выполнение методики позволило выявить каждую из внесенных аномалий. На основе результатов методики первоначальная политика корректировалась, после чего методика применялась снова, и новая политика была признана свободной от аномалий «затенения». Проведенные эксперименты по моделированию систем с большим количеством вовлеченных объектов, ролей, типов данных и правил разрешения/запрета подтверждают эффективность предложенной методики для систем индустриального уровня.

Прототипы компонентов активного аудита были реализованы в среде Rapid Miner 5.2 с целью анализа исполняемых файлов на предмет наличия вредоносного программного обеспечения на базе статической позиционно-зависимой модели объектов формата PE32. Практические работы по проверке методики обнаружения, основанной на статической позиционно-зависимой модели представления, показали, что показатель точности обнаружения AUC (площадь ROC-кривой) достигает значения 0.98 при использовании классификатора, обученного на пространстве из 250 признаков. Результаты сравнимы с результатами оценивания существующих быстрых статических методик обнаружения вредоносного программного обеспечения, основанных на использовании n-грамм и простых подходах анализа кода (дизассемблирования). Показатели точности могут быть улучшены при дальнейшем расширении пространства признаков. С точки зрения характеристик времени обучения (принятия решения) и ресурсопотребления данный подход выгодно отличается в лучшую сторону за счет ограничения потенциально возможного количества признаков, определяемым комбинацией значения и его смещения.

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Оценивание защищенности в автоматизированных системах управления РЖД

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Оценивание защищенности в автоматизированных системах управления РЖД

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

132-133

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Предлагается подход, основанный на отражении текущего уровня защищенности системы в виде набора показателей защищенности. При разработке подхода к оцениванию защищенности учитывались следующие требования, основанные на общих требованиях к системам оценивания защищенности и особенностях промышленных систем: показатели должны быть значимыми, объективными и повторяемыми; показатели должны указывать на уязвимые места системы; показатели должны определять вероятность успешной атаки и ее возможные последствия; показатели должны определять профиль нарушителя, его цели, местоположение в

системе и возможности; показатели должны учитывать текущую ситуацию на основе событий, поступающих от системы управления информацией и событиями безопасности; подход к оцениванию защищенности должен помогать принимать эффективные решения по безопасности; подход должен учитывать требования действующих стандартов и протоколов безопасности; алгоритмы вычисления показателей должны быть эффективными (вычисление должно производиться во времени, близком к реальному, что особенно важно для промышленных систем) и отражать реальное состояние защищенности информационной системы.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Поддержка принятия решений по выбору защитных мер в информационных системах на основе комплекса показателей защищенности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

132

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В рамках работы предлагается проактивный подход к выбору защитных мер, основанный на системе показателей защищенности. Подход позволяет учитывать информацию о событиях безопасности, обнаруженных в системе, и на основе спрогнозированного профиля атаки выбрать из списка защитных мер наиболее эффективные меры ее предотвращения. Данный подход является расширением предыдущей работы по анализу защищенности, в рамках которой был предложен подход к оцениванию защищенности на основе

многоуровневой системы показателей. В систему показателей защищенности добавляется новый уровень принятия решений, содержащий различные показатели оценки эффективности защитных мер.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Методы интеграции баз уязвимостей для улучшения анализа защищенности компьютерных систем

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Методы интеграции баз уязвимостей для улучшения анализа защищенности компьютерных систем

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

165-166

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В ходе работы в исследуемых базах уязвимостей были выявлены необходимые элементы для качественного анализа защищенности компьютерных систем и разработаны методы интеграции информации из данных баз, а именно: метод интеграции записей уязвимостей, метод интеграции записей продуктов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Обзор механизмов корреляции событий безопасности в SIEM-системах

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Обзор механизмов корреляции событий безопасности в SIEM-системах

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

166

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Углубленная классификация механизмов корреляции дает понять, что их существует огромное количество, а их экспериментальная эффективность уже оценена экспертами в данной области. В работе приводятся механизмы, использующие построенные векторы в заранее построенной матрице событий, основанные на представлении модели в виде объектов, и применяющие визуализацию, для наиболее удобного отображения текущего состояния системы, чтобы администратор мог оперативно и правильно принять решение.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Агеев Сергей Александрович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Оценка и управление рисками информационной безопасности в защищенных мультисервисных сетях на основе методов искусственного интеллекта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

116-117

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Важнейшей проблемой при создании и эксплуатации защищенных мультисервисных сетей (ЗМС) является проблема обеспечения их безопасного функционирования и безопасности циркулирующей в них информации. Одной из основных проблем управления безопасностью ЗМС является задача оценки и управления рисками информационной безопасности (ИБ). Оценивание риска является итерационным процессом, который заключается в оценке величины рисков, выработке мер по их уменьшению и убеждении, что риски

допустимы. На начальном этапе методом экспертной оценки решаются общие вопросы проведения оценивания риска. Вначале производится синтез модели угроз ИБ ЗМС. Далее выбираются компоненты ЗМС и степень детальности их рассмотрения. Выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности ЗМС.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Поддержка принятия решений по безопасности информации в АСУ железнодорожного транспорта на основе онтологического моделирования данных

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

144

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе описывается одно из направлений решения проблемы обеспечения безопасности информации (БИ) в АСУ железнодорожного транспорта, которое заключается в создание развитой системы управления и мониторинга комплексной безопасностью ЖТ, в частности, на концепции«управления информацией и событиями безопасности» (Security Information and Event Management). Одной из важнейших задач, решаемых в такой системе, является поддержка принятия решений на основе анализа данных о событиях безопасности, в

ходе которого проводится оценке метрик защищенности, оценка издержек, связанных с реализацией возможных контрмер и выбор наиболее приемлемых решений по обеспечению информационной безопасности. Предлагается для этой цели использовать онтологическое моделирование данных, заключающееся в построении и использовании онтологии.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Модели и методы визуального анализа больших объемов данных и событий безопасности автоматизированных систем железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

143

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается одно из направлений решения проблемы обеспечения безопасности информации (БИ) в АСУ железнодорожного транспорта, которое заключается в создание развитой системы управления и мониторинга комплексной безопасностью ЖТ, в частности, на концепции«управления информацией и событиями безопасности» (Security Information and Event Management). Одной из важнейших задач, решаемых в такой системе, является поддержка принятия решений на основе анализа данных о событиях безопасности, в

ходе которого проводится оценке метрик защищенности, оценка издержек, связанных с реализацией возможных контрмер и выбор наиболее приемлемых решений по обеспечению информационной безопасности. Предлагается для этой цели использовать онтологическое моделирование данных, заключающееся в построении и использовании онтологии.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Построение классификационной схемы существующих методов корреляции событий безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Левшун Дмитрий Сергеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Построение классификационной схемы существующих методов корреляции событий безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции. СПб., 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

148-149

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается процесс корреляции событий безопасности и его фазы. Рассматривается вопрос необходимости построения классификационной схемы существующих методов корреляции событий безопасности. Предлагается подход к классификации на основе выделения различных атрибутов методов корреляции событий.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Решение задачи формирования списков информационных объектов и их связей для визуализации данных при мониторинге и управлении информационной безопасностью

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Брюханов А.В.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Архипов Ю.А., Лепнев П.А., Чечулин А.А., Котенко И.В.

9.4 Название публикации (на языке оригинала)

Решение задачи формирования списков информационных объектов и их связей для визуализации данных при мониторинге и управлении информационной безопасностью

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы научно-технической конференции и выставки инновационных проектов «Инновации Северо-Запада». 15-16 декабря 2014 года. Санкт-Петербург

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

65-69

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство СПбГЭТУ «ЛЭТИ»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается основные принципы и источники исходных данных для проведения экспериментов с экспериментальным образцом программного обеспечения, предназначенном для визуализации данных при мониторинге и управлении информационной безопасностью.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Методика анализа истории событий безопасности, прогнозирования действий нарушителя и их последствий

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич, Дойникова Елена Владимировна

9.4 Название публикации (на языке оригинала)

Методика анализа истории событий безопасности, прогнозирования действий нарушителя и их последствий

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы научно-технической конференции и выставки инновационных проектов «Инновации Северо-Запада». 15-16 декабря 2014 года. Санкт-Петербург

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

69-72

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство СПбГЭТУ «ЛЭТИ»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается методика анализа событий безопасности и прогнозирования действий нарушителя на их основе. Методика включает статический и динамический режимы работы. На основе результатов анализа принимаются решения по безопасности.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Бушуев Сергей Николаевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Копчак Ян Миланович, Ногин Сергей Борисович, Десницкий Василий Алексеевич

9.4 Название публикации (на языке оригинала)

Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

73-77

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Изд-во СПбГЭТУ «ЛЭТИ»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Технология разработки и анализа компонентов защиты информационно-телекоммуникационных систем концепции Интернет вещей включает совокупность решений проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем, реализующих концепцию Интернет вещей. Разработаны основные принципы и методические подходы в области проектирования, верификации и тестирования компонентов защиты информационно-телекоммуникационных систем в рамках концепции

Интернет вещей. Разработаны математические модели информационно-телекоммуникационных систем и компонентов защиты в рамках концепции Интернет вещей, отражающие их основные характеристики, в том числе сетевую топологию, используемое программно-аппаратное обеспечение, конфигурацию системы защиты и учитывающих особенности устройств, специфичных для концепции Интернет вещей на основе сформированных принципов и методических подходов в области проектирования, верификации, тестирования. Разработана математическая модель нарушителя, отражающая основные его характеристики, в том числе тип, начальные возможности и права в системе, квалификацию, цели и мотивы на основе сформированных принципов и методических подходов в области проектирования, верификации, тестирования и анализа сценариев применения.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Основы технологии агрегации, нормализации и анализа данных для мониторинга безопасности сетей «Интернет вещей»

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Безродный Игорь Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Смирнов Дмитрий Борисович, Саенко Игорь Борисович, Котенко Игорь Витальевич, Волков Алексей Анатольевич

9.4 Название публикации (на языке оригинала)

Основы технологии агрегации, нормализации и анализа данных для мониторинга безопасности сетей «Интернет вещей»

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

77-81

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Технология агрегации, нормализации и анализа данных мониторинга безопасности сетей «Интернет вещей» включает совокупность решений по методам, архитектуре и средствам реализации системы мониторинга

безопасности сетей «Интернет вещей». Рассмотрена архитектура системы, реализующей данную технологию, и дана характеристика ее подсистем: сбора данных, отказоустойчивой доставки данных, масштабируемой предварительной обработки данных, гибридного онтологического хранения данных и визуализации данных.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Программно-аппаратный стенд генерации наборов тестовых гетерогенных данных для моделирования сети «Интернет вещей»

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Полушин Владимир Юрьевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Малоземов Дмитрий Геннадьевич, Саенко Игорь Борисович, Чечулин Андрей Алексеевич, Зорохович Сергей Витальевич

9.4 Название публикации (на языке оригинала)

Программно-аппаратный стенд генерации наборов тестовых гетерогенных данных для моделирования сети «Интернет вещей»

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Научно-техническая конференция «Инновации Северо-Запада». Материалы конференции. 15-16 декабря 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

81-85

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Программно-аппаратный стенд осуществляет генерацию наборов тестовых гетерогенных данных о событиях безопасности. Рассмотрены основные характеристики данного стенда, касающиеся аппаратного и

программного обеспечения, включая специальные средства анализа сетевого трафика и имитации действий нарушителя.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - A Genetic Approach for Virtual Computer Network Design

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Saenko I.

9.4 Название публикации (на языке оригинала)

A Genetic Approach for Virtual Computer Network Design

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Intelligent Distributed Computing VIII. Studies in Computational Intelligence. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

570

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

95-105

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Berlin, Heidelberg

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Одним из возможных уровней защиты информации может являться разделение компьютерной сети на логические фрагменты, которые известны как виртуальные компьютерные сети, или виртуальные подсети. Статье рассматривает новый подход к определению виртуальных подсетей, который основан на учете заданной матрицы логической связности компьютеров. Показано, что рассматриваемая проблема представляет собой одну из форм булевой матричной факторизации. Она формирует задачу проектирования виртуальных подсетей и предлагает использовать генетический алгоритм как средство ее решения. Основные

усовершенствования, предложенные в статье, заключаются в использовании тривиальных решений для генерации начальной популяции, учете в функции пригодности критерия минимального числа подсетей и использовании столбцов матрицы связности в качестве генов хромосом. Эксперименты показали, что предложенный генетический алгоритм имеет высокую эффективность.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

17

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Dynamical Attack Simulation for Security Information and Event Management

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Shorov A., Chechulin A., Novikova E.

9.4 Название публикации (на языке оригинала)

Dynamical Attack Simulation for Security Information and Event Management

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

219-234

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Heidelberg

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе представляется подход к динамическому моделированию атак и механизмов защиты, предназначенный для использования в системах управления информационной безопасностью (SIEM-системы). Для демонстрации подхода разработан прототип компонента и проведены эксперименты.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

15

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Logical Inference Framework for Security Management in Geographical Information Systems

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Polubelova O.Saenko I.

9.4 Название публикации (на языке оригинала)

Logical Inference Framework for Security Management in Geographical Information Systems

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

V. Popovich et al. (eds.), Information Fusion and Geographic Information Systems (IF&GIS 2013), Lecture Notes in Geoinformation and Cartography, DOI: 10.1007/978-3-642-31833-7_14

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

203-218

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Heidelberg

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Разработка программных средств реализации логического вывода на основе знаний о безопасности информации и событий является перспективным направлением исследований для обеспечения безопасности в крупных информационных системах, включая распределенные геоинформационные системы. Платформы, которые используют логические языки и системы логического вывода, предоставляют администраторам мощные и гибкие средства, которые обеспечивают верификацию политик безопасности, создание эффективных контрмер против компьютерных атак и поддержание требуемого уровня безопасности. В статье

излагается новый подход для разработки и осуществления системы логического вывода для управления информацией и событий безопасности. Рассматриваются общая архитектура этой системы, а также детали архитектуры и реализация конкретных модулей логического вывода, основанные на исчислении событий, методе «проверки на моделях» и онтологическом представлении данных в репозитории.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

30

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Security metrics based on attack graphs for the Olympic Games scenario

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Doynikova E., Chechulin A.

9.4 Название публикации (на языке оригинала)

Security metrics based on attack graphs for the Olympic Games scenario

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «pp.», «p» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

IEEE Computer Society

9.12.2 Город, где расположено издательство

Вашингтон

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Анализ угроз безопасности и расчет показателей защищенности является важной задачей систем мониторинга и управления информационной безопасностью. В статье рассматривается методика расчета показателей безопасности на базе графов атак и зависимостей сервисов. Методика использует несколько аспектов оценки или уровней предметной области (топологический, уровень графа атак, уровень злоумышленника, уровень событий и уровень системы) и позволяет осуществлять настройку в соответствии с различными параметрами работы системы мониторинга и управления информационной безопасностью. Рассматривается также

применение этой методики для предметной области "Олимпийских игр".

9.14 Общее число ссылок в списке использованной литературы (цифрами)

33

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Creation of a Fuzzy Knowledge Base for Adaptive Security Systems

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Nesteruk P.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Nesteruk L., Kotenko I.

9.4 Название публикации (на языке оригинала)

Creation of a Fuzzy Knowledge Base for Adaptive Security Systems

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Proceedings of the 22th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2014). Turin, Italy. 12th - 14th February, 2014.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

не заполнено

9.12.2 Город, где расположено издательство

Вашингтон

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Для создания следующего поколения адаптивных систем безопасности должны быть разработаны мощные интеллектуальные компоненты. В статье описывается нечеткая база знаний, специфицирующая связи между угрозами и механизмами защиты. Создание этой нечеткой базы знаний осуществляется с использованием Fuzzy Logic Toolbox пакета Mathworks MATLAB. Цель состоит в том, чтобы повысить эффективность реакций системы защиты на различные угрозы путем минимизации весов нейронных сетей. В статье демонстрируется методика создания такой нечеткой базы знаний для улучшения эффективности механизмов защиты на основе

мониторинга и коррекции правил защиты.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

15

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Security Assessment of Computer Networks based on Attack Graphs and Security Events

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Doynikova E.

9.4 Название публикации (на языке оригинала)

Security Assessment of Computer Networks based on Attack Graphs and Security Events

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Proceedings of the 2014 Asian Conference on Availability, Reliability and Security - AsiaARES'2014. In conjunction with ICT-EurAsia 2014. April 14th – 17th, 2014, Bali, Indonesia. / Linawati et al. (Eds.): ICT-EurAsia 2014, Lecture Notes in Computer Science (LNCS)

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

462-471

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Оценивание защищенности является важной задачей для современных компьютерных сетей. В статье предлагается методика оценивания защищенности на основе графов атак, применимая в современных системах управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Она основана на таксономии показателей защищенности и различных методиках вычисления показателей защищенности, отличающихся в зависимости от данных о текущих событиях безопасности.

Предлагаемые показатели формируют основу для отслеживания ситуации по защищенности, и позволяют отразить текущую ситуацию, в том числе развитие атак, источники и цели атак, характеристики атакующих. Продемонстрировано применение предложенной методики на тестовом примере.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

22

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Chechulin A., Shorov A., Komashinsky D.

9.4 Название публикации (на языке оригинала)

Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Lecture Notes in Artificial Intelligence (LNAI). Proceedings of the 14th Industrial Conference on Data Mining (ICDM 2014), July 16 – 21, 2014, St. Petersburg, Russia

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

39-54

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматривается проблема автоматической категоризации веб-сайтов для систем, используемых для блокировки веб-страниц, содержащих неприемлемое содержимое. Авторы применяют методики анализа текста, html тэгов, URL адресов и другой информации методами машинного обучения и интеллектуального анализа данных (Data Mining). Кроме того, предлагаются методики анализа сайтов, предоставляющих информацию на разных языках. Представлена архитектура и алгоритмы системы сбора, хранения и анализа данных, требующихся для классификации сайтов по определенным категориям. Также представлены

результаты экспериментов по анализу веб-сайтов разных категорий. Выполнена оценка качества классификации. Разработанная по результатом данной работы система классификации реализована в системах анализа веб-содержимого F-Secure.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

31

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Security Evaluation Models for Cyber Situational Awareness

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Doynikova E.

9.4 Название публикации (на языке оригинала)

Security Evaluation Models for Cyber Situational Awareness

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Proceedings of the 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS 2014). August 20-22, 2014, Paris, France

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

1229-1236

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

IEEE Computer Society

9.12.2 Город, где расположено издательство

Los Alamitos, California

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматриваются методики измерения и вычисления показателей защищенности на основе графов атак и зависимостей сервисов. Методики основаны на нескольких уровнях оценивания (топологическом, графа атак, атакующего, событий и системы) и таких важных аспектах, как атаки нулевого дня и стоимостные характеристики атак. Они позволяют оценить текущую ситуацию по защищенности, в том числе определить уязвимые и слабые места системы, выявить опасные события, параметры проходящих и возможных кибер-атак, намерения атакующих, вычислить интегральные показатели защищенности и определить возможные

защитные меры.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

34

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Visualization of Security Metrics for Cyber Situation Awareness

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Novikova E.

9.4 Название публикации (на языке оригинала)

Visualization of Security Metrics for Cyber Situation Awareness

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

The 1st International Software Assurance Workshop (SAW 2014). In conjunction with the 9th International Conference on Availability, Reliability and Security (ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. 2014

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

506-513

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

IEEE Computer Society

9.12.2 Город, где расположено издательство

Los Alamitos, California

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Одним из важных направлений исследований в области ситуационной осведомленности является реализация методов визуальной аналитики, которые могут быть эффективно применены при работе с большими данных по безопасности в критических приложениях. В статье рассматривается методика визуальной аналитики для отображения множества метрик безопасности, используемых для оценки общего состояния безопасности сети и оценки эффективности механизмов защиты. Методика призвана помочь в решении задач в области

безопасности, которые важны для систем мониторинга управления событиями (SIEM). Предложенный подход подходит для отображения показателей безопасности больших сетей и поддерживает исторический анализ данных. Чтобы продемонстрировать и оценить полезность предложенной методики был реализован прототип приложения для сценария Олимпийских игр.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

30

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Novikova E.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Kotenko I.

9.4 Название публикации (на языке оригинала)

Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS)

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

8708

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

63-78

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Berlin

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Мобильные сервисы денежных переводов (МСДП) в настоящее время развернуты на многих рынках по всему миру и широко используется для внутренних и международных денежных переводов. Тем не менее, они могут быть использованы для отмывания денег и других незаконных финансовых операций. В статье рассматривается интерактивный подход, который позволяет представить поведение абонентов МСДП в соответствии с их деятельностью по выполнению транзакций. Предложенное визуальное представление о поведении пользователей МСДП, основанное на методике визуализации RadViz, помогает определить группы

с аналогичным поведением и выбросы. Рассматривается несколько приложений, соответствующих отмыванию денег и мошенничеству. Они используются для оценки эффективности предложенного подхода, а также для представления и обсуждения результатов экспериментов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

33

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Desnitsky V.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Kotenko I.

9.4 Название публикации (на языке оригинала)

Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Proceedings of 4rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). September 8-12, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

8708

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

194-210

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Berlin

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Повышенная сложность проектирования современных защищенных систем со встроенными устройствами обуславливается низкой структуризацией и формализацией области знаний информационной безопасности. В работе предлагается подход к выявлению экспертных знаний в данной области для последующего их использования в рамках автоматизированного проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами. Разработанная методика построена на основе предметно-ориентированного анализа нескольких индустриальных систем и характеризуется заложенной в нее

специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. В работе основное внимание уделяется методике проектирования и верификации информационно-телекоммуникационных систем со встроенными устройствами с использованием экспертных знаний об аппаратных ресурсах встроенных устройств, типовых конфликтах и аномалиях, возникающих в системе. К особенностям методики можно также отнести использование метода проверки на модели для верификации сетевых информационных потоков.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

35

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Doynikova E.

9.4 Название публикации (на языке оригинала)

Evaluation of Computer Network Security based on Attack Graphs and Security Event Processing

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

5

9.10.2 Номер издания/Выпуск (арабскими цифрами)

3

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

14-29

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Innovative Information Science & Technology Research Group (ISYOU)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматривается проблема оценивания защищенности. Предлагается подход к оцениванию защищенности на основе графов атак, который может применяться в системах управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Ключевой особенностью подхода является применение разработанной системы показателей защищенности, основанной на классификации входных данных, используемых для вычисления показателей. Входные данные включают в том числе информацию о событиях безопасности от SIEM-системы. Предлагаемые показатели создают основу для отслеживания ситуации по защищенности системы путем отражения развития атак, их источников и

целей, и характеристик атакующих. Демонстрируется применение предложенной методики на тестовом примере.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

25

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Saenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Kotenko I.

9.4 Название публикации (на языке оригинала)

Design of Virtual Local Area Network Scheme based on Genetic Optimization and Visual Analysis

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

5

9.10.2 Номер издания/Выпуск (арабскими цифрами)

4

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)

9.12.2 Город, где расположено издательство

Seoul, Republic of Korea

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассатривается подход к генетической оптимизации схемы виртуальной локальной вычислительной сети с использованием разработанного инструментария – средства проектирования схемы VLAN. Авторы предлагают формальную постановку задачи оптимизации схемы VLAN, решение которой может улучшить надежность и безопасность функционирования корпоративной компьютерной сети. В статье показано, что рассматриваемая проблема является одной из форм булевой матричной факторизации. В предложенном генетическом алгоритме был реализован ряд усовершенствований, касающихся формирования начальной популяции, вида функции пригодности, кодирования хромосом и выполнения операций скрещивания и

мутации. Средство проектирования схемы VLAN позволяет решать проблему с помощью генетического алгоритма, формировать визуальное представление хода решения задачи и обеспечивает оценку генетического алгоритма. Экспериментальные результаты подтвердили высокую эффективность предложенного генетического алгоритма.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - The Framework for Simulation of Bio-inspired Security Mechanisms Against Network Infrastructure Attacks

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Shorov A.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Kotenko I.

9.4 Название публикации (на языке оригинала)

The Framework for Simulation of Bio-inspired Security Mechanisms Against Network Infrastructure Attacks

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

The Scientific World Journal. Article ID 172583

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

1-11

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Hindawi Publishing Corporation

9.12.2 Город, где расположено издательство

New York

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье представляется биоинспирированный подход под названием " нервная система сети " и методы моделирования инфраструктурных атак и механизмов защиты, основанных на предлагаемом подходе. Механизмы защиты на основе этого подхода включают распределенные процедуры сбора и обработки информации, которые координируют деятельность основных устройств компьютерной сети, идентифицируют атаки и определяют необходимые контрмеры. Атаки и механизмы защиты специфицируются в виде структурных моделей на основе теоретико-множественного подхода. Демонстрируется среда моделирования механизмов защиты, основанных на биологической метафоре, описываются эксперименты, показывающие

эффективность механизмов защиты.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

26

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Creating New Generation Cybersecurity Monitoring and Management Systems

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Saenko I.

9.4 Название публикации (на языке оригинала)

Creating New Generation Cybersecurity Monitoring and Management Systems

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Herald of the Russian Academy of Sciences

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

84

9.10.2 Номер издания/Выпуск (арабскими цифрами)

6

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

993–1001

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Pleiades Publishing, Ltd.

9.12.2 Город, где расположено издательство

Moscow

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматривается технология управления событиями и информацией безопасности – новое интенсивно развивающееся направление в области кибербезопасности, которое обладает достаточно большим потенциалом как в отношении обнаружения угроз, так и с точки зрения выработки контрмер, обеспечивающих требуемый уровень безопасности информационных инфраструктур. Системы мониторинга и управления кибербезопасностью, ориентированные на эту технологию, предполагают оперативный сбор, хранение и последующую аналитическую обработку данных о событиях, связанных с безопасностью.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

16

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Simulation of bio-inspired security mechanisms against network infrastructure attacks

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Шоров Андрей Владимирович

9.4 Название публикации (на языке оригинала)

Simulation of bio-inspired security mechanisms against network infrastructure attacks

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Intelligent Distributed Computing VIII. Studies in Computational Intelligence, Vol.570. Proceedings of 8th International Symposium on Intelligent Distributed Computing - IDC'2014. September 3-5, 2014, Madrid, Spain

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

570

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

127-133

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Springer-Verlag

9.12.2 Город, где расположено издательство

Berlin

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматривается развитие подхода к моделированию механизмов защиты от инфраструктурных атак на основе биологической метафоры. Представлена спецификация модели атак и механизмов защиты дается. Предложены алгоритмы реализации атак и механизмов защиты. Детально рассмотрена среда для моделирования механизмов безопасности на основе биологической метафоры, представлены эксперименты, которые демонстрируют возможности разработанной системы моделирования.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

21

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Предложения по онтологическому представлению и гибридному хранению данных о событиях безопасности в АСУ железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко И.В.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко И.Б.

9.4 Название публикации (на языке оригинала)

Предложения по онтологическому представлению и гибридному хранению данных о событиях безопасности в АСУ железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Технические науки — от теории к практике

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

29

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

28-32

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство «СибАК»

9.12.2 Город, где расположено издательство

Новосибирск

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье приводится описание гибридного онтологического подхода к построению информационного хранилища для системы управления и мониторинга комплексной безопасностью в АСУ железнодорожного транспорта. Рассматривается задача онтологического моделирования предметной области комплексной безопасности на транспорте. Предлагаются принципы построения архитектуры гибридного онтологического информационного хранилища. Обсуждаются результаты его реализации и использования при моделировании атак.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

7

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Предложения по реализации логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Естественные и математические науки в современном мире

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

14

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

46-50

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

НП "СибАК"

9.12.2 Город, где расположено издательство

Новосибирск

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье приводится описание обобщенной архитектуры системы логического вывода для управления кибербезопасностью в АСУ железнодорожного транспорта. Приводится характеристика отдельных модулей данной системы и реализованных в ней механизмов логического вывода – исчисления событий и метода «проверки на модели». Обсуждаются входные данные и этапы алгоритма реализации метода «проверки на модели».

9.14 Общее число ссылок в списке использованной литературы (цифрами)

8

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Методика верификации политик безопасности в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Технические науки - от теории к практике

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

30

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

18-22

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

НП "СибАК"

9.12.2 Город, где расположено издательство

Новосибирск

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье приводится описание методики верификации политик безопасности, применяемых в многоуровневой интеллектуальной системе обеспечения комплексной безопасности железнодорожного транспорта. Рассматриваются этапы методики, основанной на методе «проверки на модели». Обсуждаются вопросы построения модели компьютерной сети, модели аномалий и модели переходов, используемых в методике верификации.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

6

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальеви

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович, Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Проактивное управление информацией и событиями безопасности в информационно-телекоммуникационных системах

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Вопросы радиоэлектроники . Серия СОИУ

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

1

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

170–180

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО «ЦНИИ «Электроника 2014»

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматриваются вопросы построения проактивных систем управления и мониторинга безопасности информации для современных информационно-телекоммуникационных систем. Обсуждаются решения, полученные в ключевых областях, связанных с построением репозитория и анализом событий безопасности на основе моделирования сетевых атак.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

7

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Построение графов атак для анализа событий безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин А.А.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко И.В.

9.4 Название публикации (на языке оригинала)

Построение графов атак для анализа событий безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Безопасность информационных технологий

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации (ВНИИПВТИ)

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В настоящей работе предложен подход к использованию системы моделирования атак для повышения точности и оперативности обнаружения атак в общем потоке событий. Рассмотренные в статье задачи являются составными элементами общей системы управления инцидентами и событиями. Кроме того, предложенный подход позволяет после обнаружения атаки вычислить вероятные характеристики нарушителя (такие как, уровень знаний, технические возможности, цели, и т.д.), предсказать возможные направления развития атаки и возможные действия нарушителя, которые предшествовали проведению основной атаки

(захват управления над сетевым оборудованием, кража паролей и т.д.). Результатом работы системы моделирования атак также могут быть следующие характеристики: (1) слабые места в топологии сети (хосты, через которые проходит наибольшее число графов атак); (2) выбранные контрмеры, позволяющие снизить вероятность максимального количества графов атак; (3) возможные последствия реализации контрмер, учитывающие зависимости сервисов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

9

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Дойникова Елена Владимировна

9.4 Название публикации (на языке оригинала)

Вычисление и анализ показателей защищенности на основе графов атак и зависимостей сервисов

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Проблемы информационной безопасности. Компьютерные системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

19-36

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ГОУ «Санкт-Петербургский государственный политехнический университет»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Вычисление и анализ показателей защищенности компьютерной системы (сети) является важной задачей для систем мониторинга и управления безопасностью (Security Information and Events Management, SIEM). Ее решение позволяет определить текущую ситуацию по безопасности и необходимые контрмеры. В статье предлагается методика вычисления показателей защищенности на основе графов атак и зависимостей сервисов. Методика охватывает несколько аспектов оценивания (анализ атак и принимаемых контрмер, учет известных уязвимостей и уязвимостей “нулевого дня”, расчет стоимостных и других показателей), различные уровни представления компьютерной системы (топологический, графа атак, атакующего, событий и системы),

а также позволяет изменять применяемые алгоритмы расчета показателей защищенности в зависимости от режима функционирования SIEM-системы. Демонстрируется пример применения предложенной методики для сценария “Олимпийские Игры”.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

42

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Проектирование и верификация защищенных систем со встроенными устройствами на основе экспертных знаний

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Проектирование и верификация защищенных систем со встроенными устройствами на основе экспертных знаний

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Проблемы информационной безопасности. Компьютерные системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

3

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

16-22

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Санкт-Петербургский государственный политехнический университет (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье предложена методика проектирования и верификации информационных систем со встроенными устройствами, которая ориентирована на разработку и комплексный анализ защищенности комбинированных механизмов защиты встроенных устройств с учетом показателей ресурсопотребления, скрытых конфликтов и аномалий компонентов защиты и информационных потоков. К особенностям методики можно отнести использование специализированных эвристических знаний в области безопасности встроенных устройств в качестве готовых паттернов проектирования и верификации.

Основные результаты, представленные в статье, включают следующие стадии разработанной методики: конфигурирование компонентов защиты встроенного устройства, выявление скрытых конфликтов между компонентами защиты, верификация сетевых информационных потоков. Разработанный программный прототип включает средство принятия решений о выборе оптимальных конфигураций на этапе проектирования устройств на основе свойств имеющихся компонентов защиты и ограничений и средство верификации сетевых информационных потоков на основе метода "проверка на модели".

9.14 Общее число ссылок в списке использованной литературы (цифрами)

7

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Проблемы информационной безопасности. Компьютерные системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

3

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

56-59

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ГОУ «Санкт-Петербургский государственный политехнический университет»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье представлен подход, позволяющий использовать аналитическое моделирование атак в системах защиты информации, работающих в режиме, близком к реальному времени.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

8

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Проблемы информационной безопасности. Компьютерные системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в продолжающемся издании

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

3

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

131-135

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный политехнический университет"

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье представлен анализ открытых баз данных уязвимостей. Приведена статистика и выявлены тенденции обнаружения уязвимостей в программно-аппаратном обеспечении основных разработчиков.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

7

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - К новому поколению систем мониторинга и управления безопасностью

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

К новому поколению систем мониторинга и управления безопасностью

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Вестник Российской академии наук

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

84

9.10.2 Номер издания/Выпуск (арабскими цифрами)

11

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

993-1001

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

MAIK Nauka/Interperiodica

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье обобщены основные результаты проекта MASSIF по построению систем управления событиями и информацией безопасности, а также рассмотрены возможные сценарии применения этих разработок.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

16

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Юсупов Рафаэль Мидхатович

9.4 Название публикации (на языке оригинала)

Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XVII-я Всероссийская научно-практическая конференция "Актуальные проблемы защиты и безопасности"

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

3

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

7-18

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Санкт-Петербургский государственный политехнический университет

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Обоснована технологическая необходимость разработки нового поколения систем мониторинга и управления инцидентами безопасности, основанных на технологии управления информацией и событиями безопасности. Приведены типовая архитектура и основные решения по построению отдельных модулей таких систем, осуществляющих устойчивый сбор данных о событиях безопасности, их универсальную трансляцию, масштабируемую обработку, гибридное онтологическое хранение и многофункциональную визуализацию, а также межуровневую корреляцию событий, моделирование атак и прогностический анализ безопасности.

Сформулированы предложения по применению таких систем в предметных областях, касающихся обеспечения безопасности в критических инфраструктурах.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

25

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Построение интегрированной базы данных уязвимостей

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Построение интегрированной базы данных уязвимостей

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Известия высших учебных заведений. Приборостроение

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в продолжающемся издании

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

57

9.10.2 Номер издания/Выпуск (арабскими цифрами)

11

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

62-67

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики"

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Представлены результаты исследования открытых баз данных уязвимостей и описание процесса их интеграции для применения в системах оценивания защищенности компьютерных сетей. Предлагаются модель процесса формирования и структура интегрированной базы уязвимостей, а также описание и анализ разработанного прототипа.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

12

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Отслеживание текущей ситуации и поддержка принятия решений по безопасности компьютерной сети на основе системы показателей защищенности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Изв. вузов. Приборостроение

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

57

9.10.2 Номер издания/Выпуск (арабскими цифрами)

10

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

72-77

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство «Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматривается подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по реагированию на инциденты безопасности, основанный на использовании предлагаемой системы показателей защищенности и разработанных моделей и алгоритмов их расчета. Ключевой особенностью подхода является учет разноплановой информации при вычислении показателей защищенности, что позволяет более точно отразить текущую ситуацию по безопасности компьютерной сети.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

17

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Использование экспертных знаний для разработки защищенных систем со встроенными устройствами

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Использование экспертных знаний для разработки защищенных систем со встроенными устройствами

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Информационные технологии и вычислительные системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

4

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

58-73

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Институт системного анализа РАН

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье предлагается подход к выявлению экспертных знаний в области информационной безопасности встроенных устройств для их дальнейшего использования разработчиками встроенных устройств, в том числе в качестве входных данных автоматизированных инструментов проектирования и верификации встроенных устройств. Разработанная методика построена на основе предметно-ориентированного анализа нескольких индустриальных систем и характеризуется заложенной в нее специфичной экспертной информацией о системных ресурсах встроенных устройств, типовых конфликтах и аномалиях. К особенностям методики можно отнести использование специализированных эвристических знаний в области безопасности встроенных

устройств в качестве готовых паттернов проектирования и верификации с применением метода проверки на модели.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

35

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Информационно-управляющие системы

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в продолжающемся издании

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

5

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

72-79

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное автономное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения"

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Произведен разбор и сравнение форматов открытых баз уязвимостей, а так же форматов словарей продуктов и показателей, характеризующих уязвимости. Собрана статистика обнаруженных уязвимостей в распространенных операционных системах и веб-браузерах, а также получено распределение уязвимых продуктов основных разработчиков программного обеспечения за последние 10 лет.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

21

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - О задачах обеспечения кибербезопасности в инфраструктурах "электронного города" на основе методов искусственного интеллекта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

О задачах обеспечения кибербезопасности в инфраструктурах "электронного города" на основе методов искусственного интеллекта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

618-622

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается концепция "Электронный город", его особенности и основные задачи. А также выделяются основные проблемы, решение которых необходимо для обеспечения кибербезопасности его инфраструктур. Авторы рассматривают возможные подходы к решению этих проблем и обсуждают отдельные результаты, полученные в ходе их решения.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Разработка системы защиты пользователей от нежелательной информации в сети Интернет

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Разработка системы защиты пользователей от нежелательной информации в сети Интернет

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

642-647

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В докладе рассматривается разработанная система классификации веб-сайтов, которая может быть использована как для систем родительского контроля, так и для поиска в интернете информации запрещенной законодательством Российской Федерации. Представлено описание разработанного подхода, включающего в себя модели, методики и алгоритмы для классификации веб-сайтов на основе методов машинного обучения. Приведены результаты экспериментов, подтверждающие возможность применения разработанного подхода в системах защиты пользователей от нежелательной информации в сети Интернет

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Применение технологии обработки больших данных для защиты сетевой инфраструктуры

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Применение технологии обработки больших данных для защиты сетевой инфраструктуры

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

614-617

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается технология "больших данных" и вопросы ее применения к проблемам анализа безопасности информационных систем. И предлагается подход к обнаружению и реагированию на атаки на основе данной технологии.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Интегрированная база данных уязвимостей в системе оценки защищенности компьютерных сетей

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Интегрированная база данных уязвимостей в системе оценки защищенности компьютерных сетей

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

638-641

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Доклад посвящен интегрированной базе данных уязвимостей, используемой в качестве компонента системы оценки защищенности компьютерных сетей. Описывается методика формирования данной базы на основе нескольких открытых баз уязвимостей, а также рассматривается её прототип и приводятся результаты проведенных экспериментов над ним.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

8

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Верификация сетевых информационных потоков систем со встроенными устройствами на основе экспертных знаний

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

596-600

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО «Концерн «ЦНИИ «Электроприбор»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Ограничения на системные ресурсы встроенных устройств определяют сложность применения существующих методов и алгоритмов, используемых традиционно для защиты персональных компьютеров и серверных станций. В результате разработка защищенных встроенных устройств требует специализированных подходов к проектированию механизмов защиты, которые могли бы обеспечить стойкость системы к атакам не только за счет дополнительных средств защиты, но и за счет особенностей архитектуры системы. Верификация информационной системы со встроенными устройствами на всех этапах проектирования, как один из путей

достижения этой цели, позволяет избежать архитектурных ошибок, которые, в свою очередь, снижают уровень защищенности всей системы. В работе предложена методика верификации информационных потоков, которая построенная на основе экспертных знаний об известных видах аномалий сетевых информационных потоков. Методика нацелена на проведение оценки защищенности разрабатываемой информационной системы со встроенными устройствами, проверки корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе заданным политикам.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

15

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

601-604

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Работа посвящена проблеме реагирования на инциденты информационной безопасности в информационных системах с учетом различной информации по безопасности. Предлагаемый в работе подход позволяет осуществлять всеобъемлющую оценку рисков и помогает администратору по безопасности принять наиболее адекватное решение по реагированию с учетом временных и стоимостных требований. Подход учитывает требования стандартов и протоколов в области информационной безопасности. Для учета различных входных

данных в процессе принятия решений предлагается применять разноуровневую систему показателей защищенности. Уровни выделяются в зависимости от учитываемой в процессе вычисления показателей информации. В том числе: информации о топологии и характеристиках сети, информации о возможных атаках в сети, основанной на уязвимостях системы, информации о возможных атакующих с учетом их положения и навыков, информации о событиях безопасности в системе с точки зрения компрометации определенных хостов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Саенко Игорь Борисович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Куваев Валерий Олегович

9.4 Название публикации (на языке оригинала)

О применении методов искусственного интеллекта для разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

631-637

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматриваются основные подходы к применению методов искусственного интеллекта с целью разграничения доступа к ресурсам единого информационного пространства разнородных автоматизированных систем. Анализируется состояние исследований в данной предметной области. Выделяются четыре группы задач по реализации этих подходов, и дается их краткая характеристика.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

14

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Агеев Сергей Александрович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Управление рисками информационной безопасности защищенной мультисервисной сети специального назначения на основе интеллектуальных мультиагентов

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы конференции "Информационные технологии в управлении" (ИТУ-2014). 7-9 октября 2014 г. СПб

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

556-562

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ОАО "Концерн "ЦНИИ "Электроприбор"

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматриваются основные подходы построения интеллектуальных методов и алгоритмов, синтезированных на их основе, оценки и управления рисками информационной безопасности защищенных мультисервисных сетей (ЗМС). Показана необходимость применения интеллектуальных методов управления ЗМС СН. Разработана и исследована математическая модель оценки риска информационной безопасности ЗМС СН.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

17

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Концептуальная комбинированная модель системы защиты встроенных устройств

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Концептуальная комбинированная модель системы защиты встроенных устройств

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Журнал «Инновации в науке»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

38

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

55-59

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство НП «СибАК»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Проектирование защищенных систем со встроенными устройствами представляет собой важнейшую задачу в области информационной безопасности. Особенностями таких систем являются автономность устройств, входящих в систему, и ограничения, накладываемые на ресурсы устройств, и вытекающая из этого их слабая производительность. Предлагаемая в работе концептуальная комбинированная модель системы защиты встроенных устройств нацелена на нахождение наиболее эффективных комбинаций компонентов защиты на основе решения оптимизационной задачи с учетом нефункциональных свойств и ограничений устройства. На основе данных об ограничениях ресурсопотребления устройств системы и требованиях к защите принимается

решение о выборе оптимальной конфигурации защиты. Верификация комбинированной системы защиты встроенных устройств проводится с использованием модели нарушителя встроенных устройств и позволяет выявить угрозы, которым подвержены устройства системы.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

4

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Разработка модели знаний для проектирования защищенных встроенных устройств

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Разработка модели знаний для проектирования защищенных встроенных устройств

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Журнал «Естественные и математические науки в современном мире»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

23

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

35-40

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство НП «СибАК»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Стремительное возрастание количества разновидностей и экземпляров встроенных устройств, их повсеместное распространение и организация в виде систем «Интернет вещей» ставят особенно остро вопросы разработки механизмов их защиты от широкого круга угроз информационной безопасности. Сложность проектирования защищенных встроенных устройств обуславливается во многом слабой структуризацией и формализацией области знаний информационной безопасности встроенных устройств. Модель знаний о безопасности встроенных устройств, включающая, требования, компоненты и настройки защиты, угрозы, а также типы и уровни возможного нарушителя в качестве системы экспертных знаний предназначена для ее

использования разработчиками встроенных устройств на этапе проектирования. В силу слабой структуризацией области знаний информационной безопасности встроенных устройств использование предложенной модели разработчиками встроенных устройств будет способствовать повышению защищенности конечных продуктов и сервисов за счет применения знаний, полученных на экспертном уровне. Использование модели знаний будет способствовать более эффективной организации процесса разработки систем защиты семейств устройств, имеющих общую базовую функциональность, но отличающихся специфичными деталями и расширениями, определяющими особенности эксплуатации устройства и его стоимость. При этом использование модели знаний в рамках каждого проблемно-предметного домена позволит сократить количество итераций и продолжительность процесса разработки за счет адаптации уже имеющихся знаний с учетом специфики конкретных устройств.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

10

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Обобщенная модель нарушителя и верификации информационно-телекоммуникационных систем со встроенными устройствами

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Журнал «Технические науки — от теории к практике»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

39

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

7-21

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство НП «СибАК»

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Сложность разработки и реализации требований к защите информационно-телекоммуникационных систем и встроенных устройств обуславливает необходимость построения моделей и методов проектирования и верификации механизмов защиты с учетом угроз информационной безопасности, целей и ресурсов возможных нарушителей, а также функциональных особенностей устройств. Предложены обобщенная модель нарушителя на основе анализа существующих классификаций нарушителей и верификация спецификаций в качестве метода тестирования защищенности устройств в процессе проектирования. Тестирование позволяет

разработчику выявить потенциальные угрозы и осуществить отбор возможных типов нарушителей в зависимости от функциональности устройств и ожидаемых сценариев использования, после чего формируется список возможных атак на это устройство. Верификация включает анализ спецификаций на предмет проверки условий, необходимых для выполнения выявленных видов атак, в том числе проверку наличия определенных аппаратных компонентов и коммуникационных интерфейсов, которые могут использоваться в качестве стартовой точки для проведения атаки.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

12

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Проактивное управление информацией и событиями безопасности в сетях NGN

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович, Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Проактивное управление информацией и событиями безопасности в сетях NGN

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы семинара Международного союза электросвязи «Переход развивающихся стран с существующих сетей на сети нового поколения (NGN): технические, экономические, законодательные и политические аспекты» 23–25 июня 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Прочие виды

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича»

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассмотрены особенности сетей NGN как объектов мониторинга и управления безопасностью. Приведена общая архитектура системы проактивного управления информацией и событиями безопасности. Обсуждались вопросы построения и функционирования основных компонентов системы, к числу которых относятся

репозиторий данных о событиях безопасности, компонента анализа защищенности и компонент визуализации.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Носков Антон Николаевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Тарасова Дарья Алексеевна

9.4 Название публикации (на языке оригинала)

Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды СПИИРАН

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Наука

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Анализ методик систем обнаружения сетевых атак является перспективным направлением в области защиты сетей и сетевых систем. В статье рассматривается подход к оценке алгоритмов и механизмов обнаружения атак. Новизна предлагаемой методики заключается в возможности создания самообучающихся систем для обнаружения вторжения. В статье рассмотрены основные элементы алгоритмов обнаружения атак.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

21

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Агеев Сергей Александрович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович, Егоров Юрий Петрович, Гладких Анатолий Афанасьевич, Богданов Александр Валентинович

9.4 Название публикации (на языке оригинала)

Интеллектуальное иерархическое управление рисками информационной безопасности в защищенных мультисервисных сетях специального назначения

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Автоматизация процессов управления

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

78-88

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ФНПЦ ОАО «НПО «Марс»

9.12.2 Город, где расположено издательство

Ульяновск

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматриваются основные подходы построения интеллектуальных методов и алгоритмов, синтезированных на их основе, оценки и управления рисками информационной безопасности защищенных мультисервисных сетей (ЗМС). Показана необходимость применения интеллектуальных методов управления ЗМС. Разработана и исследована математическая модель оценки риска информационной безопасности ЗМС.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

18

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Куваев Валерий Олегович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Проблемы экономики и управления в торговле и промышленности

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

101-104

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный торгово-экономический университет"

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье излагаются концептуальные основы интеграции неоднородных информационных ресурсов предприятия в едином информационном пространстве. Формулируются формализованные постановки задач, необходимые для эффективной интеграции информационных ресурсов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

6

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Подход к построению системы показателей качества единого информационного пространства

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Саенко Игорь Борисович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Куваев Валерий Олегович, Алышев Сергей Владимирович

9.4 Название публикации (на языке оригинала)

Подход к построению системы показателей качества единого информационного пространства

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Естественные и математические науки в современном мире

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

14

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

51-56

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство «СибАК»

9.12.2 Город, где расположено издательство

Новосибирск

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье приводится описание системы показателей качества, предназначенной для оценки единого информационного пространства. Выделяются наиболее существенные характеристики и предлагаются показатели для их оценки.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

6

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Fast Network Attack Modeling and Security Evaluation based on Attack Graphs

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Kotenko I.

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Chechulin A.

9.4 Название публикации (на языке оригинала)

Fast Network Attack Modeling and Security Evaluation based on Attack Graphs

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

EN

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Journal of Cyber Security and Mobility

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в журнале

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

3

9.10.2 Номер издания/Выпуск (арабскими цифрами)

1

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

27-46

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

River Publishers

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье предлагается подход к моделированию сетевых атак и оцениванию защищенности, применимый к системам управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Он основан на моделировании сети и поведения злоумышленников, построении графов атак, обработке текущих предупреждений для дополнения частичных графов атак в режиме, близком к реальному времени, вычислении различных показателей защищенности и предоставлении процедур оценивания защищенности. Новизна предлагаемого подхода состоит в применении особых алгоритмов построения, модификации и анализа графов атак, направленных на быструю оценку безопасности. Это позволяет использовать подход в

SIEM системах, которые функционируют в режиме, близком к реальному времени. Выделяется архитектура компонента моделирования атак и оценки защищенности (Attack Modeling and Security Evaluation Component, AMSEC), как одного из основных компонентов SIEM систем. Определны основные компоненты и методики моделирования атак и оценки защищенности. Представлен прототип AMSEC.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

37

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Модели и методики визуального анализа данных для решения задач компьютерной безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Новикова Евгения Сергеевна

9.4 Название публикации (на языке оригинала)

Модели и методики визуального анализа данных для решения задач компьютерной безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды шестнадцатой Международной конференции “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

не заполнено

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Анализируются различные модели и методики визуального анализа, разработанные для мониторинга сетевого трафика, анализа таблиц маршрутизации, оценки политик безопасности и уровня защищенности компьютерных сетей. Формулируются основные требования к подсистеме визуального анализа как составной части автоматизированных систем мониторинга и управления информационной безопасностью, предлагается общий подход к ее проектированию. Демонстрируются возможности разработанной системы визуального анализа для моделирования атак и оценки уровня защищенности.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды шестнадцатой Международной конференции “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

не заполнено

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматривается предлагаемый подход к оценке защищенности компьютерных сетей, позволяющий производить анализ поступающих событий безопасности в реальном времени. Рассмотрены основные элементы используемых моделей, алгоритмов и методик. Приведено описание разработанного программного прототипа системы и результаты экспериментов, подтверждающие достижение заявленных показателей эффективности оценки защищенности.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды шестнадцатой Международной конференции “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

не заполнено

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматриваются модели, методики и программные средства проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами, основанные на использовании экспертных знаний специалистов в области защиты информации.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды шестнадцатой Международной конференции “РусКрипто’2014”. Московская область, г.Солнечногорск, 25-28 марта 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

не заполнено

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Приводится обзор наиболее распространенных баз уязвимостей, таких как CVE, NVD и OSVDB. Анализируются их основные достоинства и недостатки с точки зрения использования этих баз при анализе защищенности компьютерной сети. Представляются результаты анализа основных тенденций в области обнаружения уязвимостей в программно-аппаратных продуктах таких компаний как Microsoft, Apple, Cisco, Google и т.д.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Интеллектуальные системы на транспорте: тезисы докладов IV международной научно-практической конференции «ИнтеллектТранс-2014»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

21

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Петербургский государственный университет путей сообщения Императора Александра I»

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье предлагается в основу построения многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем (АС) ЖТ положить технологию мониторинга и управления информационной безопасностью. Рассматриваются архитектура такой системы, исходные данные,

методы и алгоритмы функционирования системных компонентов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

О построении многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Интеллектуальные системы на транспорте: Материалы IV международной научно-практической конференции «ИнтеллектТранс-2014»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

196-203

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Петербургский государственный университет путей сообщения Императора Александра I»

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье предлагается в основу построения многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем (АС) ЖТ положить технологию мониторинга и управления информационной безопасностью. Рассматриваются архитектура такой системы, исходные данные,

методы и алгоритмы функционирования системных компонентов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Юсупов Рафаэль Мидхатович

9.4 Название публикации (на языке оригинала)

Системы мониторинга и управления кибербезопасностью нового поколения для защиты информации в критически важных инфраструктурах

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XVII-я Всероссийская научно-практическая конференция "Актуальные проблемы защиты и безопасности"

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

ЗАО "НПО Специальных материалов"

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Рассматриваются проблемы интеллектуализации защиты информации в критически-важных областях на основе построения системы интеллектуальных сервисов защиты информации (СИСЗИ) как нового и важнейшего компонента системы защиты информации в критической инфраструктуре.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

21

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Визуальная аналитика на страже информационной безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Новикова Евгения Сергеевна

9.4 Название публикации (на языке оригинала)

Визуальная аналитика на страже информационной безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Международный форум по практической безопасности Positive Hack Days. Москва. 21-22 мая 2014 г. http://www.phdays.ru

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Positive Technologies

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Методы визуальной аналитики позволяют значительно повысить эффективность администратора безопасности, так как они сочетают мощность интеллектуальных методов обработки данных и особенности зрительного восприятия информации человеком. В докладе рассматриваются существующие методы визуального анализа данных для решения различных задач защиты от компьютерных атак. Эффективность применения визуального анализа демонстрируется на примере работы разработанных авторами средств визуальной аналитики, в том числе для анализа трафика, моделирования атак, оценки защищенности,

обнаружения финансовых нарушений в системе мобильных денежных переводов и др.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Саенко Игорь Борисович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

368-373

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Академия МВД Республики Беларусь

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассматриваются основы построения перспективных систем мониторинга и управления безопасностью для защиты критически важных объектов информатизации. Приводятся основные требования к таким системам. Рассматривается обобщенная архитектура такой системы и ее компонентов. Подробнее обсуждается порядок функционирования компонента анализа защищенности и моделирования атак.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Интегрированная база данных уязвимостей

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Интегрированная база данных уязвимостей

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды Международной научно-практической конференции "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

268-272

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

УО «Академия Министерства внутренних дел Республики Беларусь»

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается вопрос объединения открытых баз данных уязвимостей с целью увеличения количества уникальных записей об уязвимостях и расширения списка продуктов, в которых они могут иметь успешную реализацию. Данный подход позволит повысить вероятность обнаружения уязвимых программно-аппаратных средств в компьютерных сетях. В работе предлагается модель интегрированной базы данных уязвимостей и прототип интегрированной базы данных. Проведена оценка эффективности прототипа.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Анализ и классификация возможных изменений, происходящих в компьютерной сети и их влияние на деревья атак

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Анализ и классификация возможных изменений, происходящих в компьютерной сети и их влияние на деревья атак

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды Международной научно-практической конференции "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

273-276

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

УО «Академия Министерства внутренних дел Республики Беларусь»

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается представление атакующих действий в компьютерной сети в виде деревьев атак и влияние изменений в компьютерной сети на модель атак и текущую ситуацию по защищенности. Для этого разработана оригинальная классификация изменений в сети и алгоритмы модификации модели атак для различных изменений.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Специфика двухуровневой организации адаптивных систем защиты информации

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Нестерук Филипп Геннадьевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Специфика двухуровневой организации адаптивных систем защиты информации

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

227-231

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Академия МВД Республики Беларусь

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассмотрены особенности организации двухуровневой организации адаптивных систем защиты информации на базе средств интеллектуального анализа данных, являющиеся базой построения многоуровневой системы адаптивной защиты. Рассмотрена специфика использования интеллектуального анализа данных при организации адаптивных уровней системы защиты информации.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Вычисление показателей защищенности в системах мониторинга и управления безопасностью

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Вычисление показателей защищенности в системах мониторинга и управления безопасностью

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды международной научно-практической конференции "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 года, г. Минск, Академия МВД Республики Беларусь

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

155-159

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Минск : Акад. МВД

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматриваются методики вычисления различных показателей защищенности в рамках систем мониторинга и управления безопасностью. Показатели позволяют оценить текущую ситуацию по безопасности и формируют основу для выбора защитных мер.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Разработка компонентов защиты встроенных устройств с учетом экспертных знаний

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Дойникова Елена Владимировна

9.4 Название публикации (на языке оригинала)

Разработка компонентов защиты встроенных устройств с учетом экспертных знаний

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Международная научно-практическая конференция "Теоретические и прикладные проблемы информационной безопасности". 19 июня 2014 г.

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

150-155

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Академия МВД Республики Беларусь

9.12.2 Город, где расположено издательство

Минск, Республика Беларусь

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В статье рассмотрены вопросы формирования, структуризации и уточнения экспертных знаний, характеризующих различные аспекты проектирования и верификации механизмов защиты встроенных устройств. Приведены результаты поиска и адаптации существующих и разработки новой методики и автоматизированного программного стенда в интересах их последующего использования разработчиками встроенных устройств.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

97-98

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В настоящее время на первое место в противодействии новым угрозам безопасности на железнодорожном транспорте (ЖТ) выдвигаются не разработка новых механизмов защиты информации, а эффективное и комплексное применение этих механизмов. Решение данной задачи предполагается возможным на основе создания и применения многоуровневой интеллектуальной системы обеспечения информационной

безопасности автоматизированных систем (АС) ЖТ. В основу построения такой системы предлагается положить технологию «управления информацией и событиями безопасности» (Security Information and Event Management, SIEM). В архитектуре предлагаемой многоуровневой интеллектуальной системы обеспечения информационной безопасности АС ЖТ выделяются три уровня: 1) уровень традиционных средств защиты (нижний); 2) уровень интеллектуальных сервисов сбора, предварительной обработки и хранения данных (средний); 3) уровень интеллектуальных сервисов анализа данных (высший).

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Особенности построения системы защиты информации в кибер-физических системах

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич, Десницкий Василий Алексеевич

9.4 Название публикации (на языке оригинала)

Особенности построения системы защиты информации в кибер-физических системах

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

67-69

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В настоящее время наблюдается стремительное развитие кибер-физических систем или т.н. Интернета вещей. Повышение сложности систем влечет за собой увеличение числа их возможных уязвимостей. Хотя, в настоящее время, многие разработчики проявляют большой интерес к механизмам защиты таких сетей, очень мало внимания уделяется устойчивости инфраструктуры к атакам, что представляет собой угрозу нормального функционирования таких систем. Современные механизмы защиты ориентированы в основном на предоставление защиты против определенных угроз и чаще всего не могут быть установлены на

специализированные устройства. В работе предлагается использовать комплексный подход к моделированию инфраструктурных атак, процессов безопасности происходящих внутри сетей кибер-физических систем. Такой подход защиты отличается от существующих аналогов ориентированностью на особенности кибер-физических систем и включает в себя методы, методики и алгоритмы, предназначенные для: (1) анализа и построения архитектуры системы защиты для кибер-физической системы, включающей в себя как центры управления безопасностью, так и сенсоры для сбора информации (2) сбора данных для построения моделей объектов и процессов характерных для конкретных кибер-физических систем; (3) выработки конкретных требований к защищенности кибер-физических систем; (4) построения аналитической модели системы, ее процессов функционирования, возможных атакующих и т.д.; (5) предварительной оценки защищенности; (6) построения модели событий безопасности влияющих как на процесс функционирования, так и на состояния отдельных объектов; (7) организации интеллектуального анализа событий безопасности в реальном времени для выявления возможных атакующих действий; (8) формирования отчета и элементов визуализации результатов работы системы безопасности.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Конфигурирование информационных систем со встроенными устройствами для обеспечения комплексной безопасности железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Конфигурирование информационных систем со встроенными устройствами для обеспечения комплексной безопасности железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

89-90

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Существующие системы поддержки процессов на железнодорожном транспорте (ЖТ) представляют собой информационно-телекоммуникационные сетевые и распределенные архитектуры, которые включают взаимодействующие между собой, как стационарные, так и мобильные подсистемы и устройства. Предлагаемая в работе модель процесса конфигурирования представляет нахождение оптимальной конфигурации компонентов защиты и основывается на получении нефункциональных показателей защиты для

решения оптимизационной экстремальной задачи при ограничениях на значения этих показателей и заданной целевой функции позволяет построить наиболее эффективную конфигурацию. Конфигурирование отличается направленностью на возникающие изменения в требованиях, вносимые на различных этапах процесса проектирования и влекущие пересмотр ранее проведенных этапов. Проектирование встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности ЖТ включает: (1) анализ моделей нарушителя, спецификацию функциональных свойств защиты и свойств программно-аппаратной совместимости; (2) задание ограничений ресурсопотребления платформы устройства; (3) поиск и формирование репозитория имеющихся компонентов защиты встроенных устройств, определение их свойств; (4) проведение анализа несовместимостей компонентов защиты с использованием экспертных знаний; (5) проведение оценки ресурсопотребления компонентов защиты при помощи автоматизированных модулей тестирования на основе эмуляции устройств; (6) выбор компонентов защиты на основе учета показателей ресурсопотребления с использованием эвристик по выбору порядка учета критериев ресурсопотребления.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Комбинированная модель защиты информационно-телекоммуникационных систем концепции «Интернет вещей»

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Комбинированная модель защиты информационно-телекоммуникационных систем концепции «Интернет вещей»

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

65-66

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Современные информационно-телекоммуникационные системы отличаются сложной распределенной структурой, разнообразием угроз информационной безопасности (ИБ) и возможных видов нарушителей ИБ, высокой динамикой внедрения новых телекоммуникационных технологий, изменением во времени сетевой топологии, одновременным использованием нескольких типов коммуникаций на основе широкополосных и беспроводных протоколов, мобильностью и автономностью входящих в нее устройств, тенденцией к

увеличению объемов обрабатываемой информации и вытекающей отсюда нехваткой вычислительных и коммуникационных ресурсов устройств. В работе исследуются новые эффективные подходы к проектированию защищенных распределенных информационно-телекоммуникационных систем в рамках концепции «Интернет вещей» на основе комбинирования средств противодействия атакам со стороны широкого класса потенциальных нарушителей. Предлагаемая модель защиты ориентирована на достижение компромисса между функционалом системы и отдельных устройств и уровнем их защищенности.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Верификация информационно-телекоммуникационных систем со встроенными устройствами на основе обобщенной модели нарушителя

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Верификация информационно-телекоммуникационных систем со встроенными устройствами на основе обобщенной модели нарушителя

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

66-67

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе представлена обобщенная модель нарушителя встроенных устройств, которая используется при разработке моделей, методов и реализующих их средств обеспечения безопасности информационно-телекоммуникационных систем со встроенными устройствами. Для определения возможных атак на встроенное устройство применяется применять аналитический подход с использованием существующих классификаций нарушителя встроенного устройства по уровню взаимодействия нарушителя с устройством

(классификация Рае и др.) и по возможностям нарушителя (классификация Гранда, классификация Абрахама). Обобщенная модель нарушителя используется для проведения верификации спецификации встроенного устройства на наличие потенциальных уязвимостей, формирования тестов физической проверки устройства, построения первоначального списка необходимых программных и программно-аппаратных компонентов защиты, которые интегрируются в устройство, а также для определения необходимого уровня защищенности от нарушителей различных типов и уровней. К недостаткам рассматриваемой модели нарушителя можно отнести отсутствие в ней классификации нарушителей по уровню доступа к администрированию устройств и системы в целом. Так, например, если пользователь имеет права администратора системы, то он может, как намеренно или так не умышленно нарушить политику безопасности системы.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Анализ уязвимостей по временным характеристикам на основе открытой базы данных X-Force

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Федорченко Андрей Владимирович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Анализ уязвимостей по временным характеристикам на основе открытой базы данных X-Force

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

104-105

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В настоящее время наиболее успешную реализацию имеют атаки, использующие уязвимости в программно-аппаратном обеспечении. В связи с данным фактом использование баз данных уязвимостей приобретает все большую актуальность, а поиском и описанием уязвимостей занимается множество организаций, компаний и исследовательских институтов. Одними из важнейших характеристик уязвимостей являются: (1) актуальность использования кода, реализующего уязвимость, (2) статус их исправления и (3) подтверждение их технических деталей. Данные характеристики являются временными, то есть могут изменяться с течением

времени. При исследовании записей базы X-Force по годам была произведена оценка основных тенденций и текущей ситуации в эксплуатации и обезвреживанию уязвимостей. На основе проведенного исследования можно сделать вывод, что вместе с сохраняющимся большим количеством детектируемых уязвимостей увеличивается и качество технической поддержки программно-аппаратного обеспечения, в котором они обнаруживаются. Это свидетельствует о повышении уровня безопасности продуктов производителями, на этапе их эксплуатации, а не на этапе разработки.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Подход к оцениванию защищенности на основе графов атак в системах управления информацией и событиями безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Подход к оцениванию защищенности на основе графов атак в системах управления информацией и событиями безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Методы и технические средства обеспечения безопасности информации. Материалы 23-й научно-технической конференции. 30 июня - 3 июля 2014 г. Санкт-Петербург

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

90-91

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается компонент оценивания защищенности и его работа в рамках систем управления информацией и событиями безопасности (Security Information and Events Management, SIEM) и методики вычисления различных показателей защищенности. Компонент оценивания защищенности позволяет повысить эффективность управления защищенностью системы. Показатели позволяют оценить текущую ситуацию по безопасности и формируют основу для выбора защитных мер.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Агеев Сергей Александрович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Интеллектуальные методы управления рисками информационной безопасности мультисервисных сетей связи

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

59-60

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Важнейшей проблемой при использовании защищенной мультисервисной сети (ЗМС) является проблема обеспечения ее безопасного функционирования и безопасности циркулирующей в ней информации. В докладе показывается, что оперативное оптимальное управление затрудняется вследствие больших размерностей совокупности решаемых задач по управлению ЗМС. Обосновывается, что многообразие, разнородность, неполнота и нечеткость исходных данных, учитываемых в задачах управления ЗМС, включая управление безопасностью, предопределяют необходимость использовать средства и методы искусственного интеллекта

для выработки рациональных (оптимальных) управленческих решений. Для решения проблемы управления безопасностью ЗМС управление рисками ЗМС и процедуры их оценки предлагается строить на основе технологии интеллектуальных мультиагентов (ИМА), основой которых является технология «агент-менеджер». Один агент отвечает за часть задания, а общее решение возникает в результате их совместного выполнения. Программное средство «менеджер/агент» управляет действиями функциональной группой агентов и может передавать агрегированную информацию на верхний уровень иерархии, которую обрабатывает программное средство «менеджер».

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Подход к решению задачи разграничения доступа в разнородном информационном пространстве

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Куваев Валерий Олегович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Подход к решению задачи разграничения доступа в разнородном информационном пространстве

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Материалы 23-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

33-34

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство Политехнического университета (Санкт-Петербург)

9.12.2 Город, где расположено издательство

не заполнено

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В современных исследованиях концепция «единого информационного пространства» (ЕИП) рассматривается как направление, определяющее дальнейшее развитие информационного обеспечения в целях создания сетеориентированных гетерогенных информационных систем коллективного пользования. Гетерогенность означает, что данные ресурсы ЕИП являются разнородными по содержанию и форматам представления и, кроме того, они могут отличаться по критериям и методам обеспечения безопасности. В результате разграничение доступа в разнородном информационном пространстве становится достаточно сложной

задачей. Для ее решения предлагается подход, основанный на двухэтапном моделировании системы разграничения доступа к ресурсам ЕИП. На первом этапе формируется концептуальная модель системы разграничения доступа в ЕИП, в которой отражаются основные понятия данной предметной области и отношения между ними. Концептуальная модель обеспечивает понятийный базис системы управления доступа. На втором этапе модель насыщается формальной семантикой за счет использования онтологического представления правил разграничения доступа в ЕИП.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Система логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

2

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

271-276

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Физматлит

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается архитектура системы логического вывода и верификации политик безопасности в автоматизированных системах железнодорожного транспорта. Обсуждаются вопросы построения модулей верификации политик безопасности, основанные на Model checking и исчислении событий, а также онтологического хранилища данных. Раскрываются аспекты реализации компонентов системы, сущность методов верификации и вопросы тестирования онтологического хранилища.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

7

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Саенко Игорь Борисович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Генетический подход к проектированию виртуальных компьютерных сетей на основе генетических алгоритмов

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT'14»

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

1

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

35-40

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Физматлит

9.12.2 Город, где расположено издательство

Москва

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе представлен новый подход к проектированию виртуальных компьютерных сетей, который принимает во внимание заданную матрицу логической связности компьютеров. Показано, что задача относится к классу булевой матричной факторизации. Для ее решения предлагается усовершенствованный генетический алгоритм. Основные новшества алгоритма связаны с использованием тривиальных решений для создания начальной популяции, учетом критерия минимального количества виртуальных подсетей в функции полезности и использованием столбцов матрицы связности в качестве генов хромосом.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

5

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Интеллектуальная система мониторинга и управления инцидентами кибербезопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Котенко Игорь Витальевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Саенко Игорь Борисович

9.4 Название публикации (на языке оригинала)

Интеллектуальная система мониторинга и управления инцидентами кибербезопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

Четырнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2014 (24–27 сентября 2014 года, г. Казань, Россия): Труды конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

3

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

219-227

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

Издательство РИЦ «Школа»

9.12.2 Город, где расположено издательство

Казань

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе представлена формальная система интеллектуальных методов мониторинга и управления инцидентами кибербезопасности, позволяющая обосновать состав и содержание данных методов. Приведено формальное описание методов, используемых на начальных этапах мониторинга кибербезопасности, и дан пример их реализации.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

10

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Анализ и применение показателей защищенности в SIEM-системах на основе графов атак и зависимостей сервисов

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Дойникова Елена Владимировна

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Анализ и применение показателей защищенности в SIEM-системах на основе графов атак и зависимостей сервисов

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013). Труды конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Статья в сборнике

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Принято в печать

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

не заполнено

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе рассматривается вычисление и применение показателей защищенности компьютерной системы (сети) для систем мониторинга и управления безопасностью (Security Information and Events Management, SIEM). На основе выделения нескольких аспектов оценивания (анализ атак и принимаемых контрмер, учет известных уязвимостей и уязвимостей “нулевого дня”, расчет стоимостных и других показателей) и различных уровней представления компьютерной системы (топологический, графа атак, атакующего, событий и системы)

сформирован подход к определению текущей ситуацию по безопасности. Предлагаемые в рамках подхода алгоритмы расчета показателей защищенности зависят от уровня представления компьютерной системы и режима функционирования SIEM-системы.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

26

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Методы определения основного языка веб-страниц

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Новожилов Дмитрий Александрович

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.4 Название публикации (на языке оригинала)

Методы определения основного языка веб-страниц

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

155-156

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Важным направлением в анализе данных является задача классификации, когда требуется отнести исследуемый объект к одному из множества заранее известных классов. Например, банковский служащий определяет, представителем какой из двух категорий: «платежеспособен» или «неплатежеспособен», - является обратившегося за кредитом клиент. Для этого производится анализ всей доступной информации и на основе результатов этого анализа принимается решение. Другой иллюстрацией решения подобной задачи может послужить функционирование системы родительского контроля, распределяющей веб-страницы по

категориям и блокирующей те из них, которые оказались нежелательными.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Решение задачи классификации сайтов на иностранных языках в сети интернет

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Комашинский Дмитрий Владимирович

9.4 Название публикации (на языке оригинала)

Решение задачи классификации сайтов на иностранных языках в сети интернет

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

169-170

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В настоящее время Интернет является одним из основных способов получения информации. Отсутствие эффективных механизмов, классифицирующих информацию и регулирующих доступ к ней в сети Интернет, создает проблему получения нежелательной, сомнительной и вредоносной информации. В первую очередь, это касается необходимости ограничения доступа к определенным видам информации по возрастным категориям. Кроме того, ограничение автоматической загрузки сайтов, принадлежащих к категориям повышенного риска (например, категории “сайты для взрослых”, “сайты с нелицензионным программным

обеспечением” и т.д.), повысит защищенность пользователей от вредоносных и нежелательных программ. Одной из важных задач является классификация сайтов на разных языках, так как модели классификаторов не могут быть эффективно обучены распознавать языковые особенности одновременно для многих языков. В данной работе рассмотрен подход, позволяющий свести задачу классификации сайтов на иностранных языках (т.е. отличных от английского) к задаче классификации англоязычных сайтов.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Программный прототип компонента аналитического моделирования атак для систем управления информацией и событиями безопасности

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Чечулин Андрей Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Программный прототип компонента аналитического моделирования атак для систем управления информацией и событиями безопасности

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

170-171

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

Одним из эффективных подходов к оценке защищенности компьютерных сетей является подход, основанный на моделировании атак. Одним из представлений, описывающим возможные действия атакующего, являются деревья атак. Узлы дерева атак могут быть представлены как возможные атакующие действия, связанные между собой в соответствии с тем, в каком порядке их может выполнять нарушитель.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Анализ перспективных систем со встроенными устройствами для формирования экспертных знаний в области проектирования защищенных информационно-телекоммуникационных систем

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

не заполнено

9.4 Название публикации (на языке оригинала)

Анализ перспективных систем со встроенными устройствами для формирования экспертных знаний в области проектирования защищенных информационно-телекоммуникационных систем

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

130

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе проводится анализ трех информационно-телекоммуникационных систем в качестве источника экспертных знаний в области проектирования защищенных систем со встроенных устройств: система удаленного автоматизированного контроля расхода электроэнергии потребителями, система устройств оперативного реагирования и управления в чрезвычайных ситуациях и система по предоставлению цифровых

мультимедиа сервисов массовому потребителю. Выбор данных систем обуславливается необходимостью охвата нескольких областей приложения, различающихся структурой, назначением, функциональными устройств и особенностями защиты. Конечная цель проводимого анализа – обобщение знаний о конкретных системах и устройствах и их последующее применение в качестве паттернов проектирования и верификации в процессе разработки новых информационно-телекоммуникационных систем.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено

Форма 509. ПУБЛИКАЦИИ ПО РЕЗУЛЬТАТАМ ПРОЕКТА - Концептуальная комбинированная модель системы защиты встроенных устройств и ее применение для конфигурирования компонентов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта

9.1 Номер проекта

13-01-00843

9.2 Первый автор (фамилия, имя, отчество)

Десницкий Василий Алексеевич

9.3 Другие авторы (для каждого - фамилия, имя, отчество)

Котенко Игорь Витальевич

9.4 Название публикации (на языке оригинала)

Концептуальная комбинированная модель системы защиты встроенных устройств и ее применение для конфигурирования компонентов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта

9.5 Язык публикации – указывается в соответствии с предоставленным списком языков

RU

9.6.1 Полное название издания (журнала, сборника и т.д.) на языке оригинала

XIV Санкт-Петербургская Международная Конференция “Региональная информатика-2014” (“РИ-2014”). Материалы конференции

9.7 Вид публикации (числовое поле; является обязательным к заполнению) (указать цифрой: 1 - монография, 2 - статья в сборнике, 3 - статья в продолжающемся издании, 4 - статья в журнале, 5 - тезисы доклада, 6 - прочие виды)

Тезисы

9.8 Завершенность публикации (указать цифрой: 1 - опубликовано; 2 - принято в печать; 3 - сдано в печать)

Опубликовано

9.9 Год публикации (арабскими цифрами, четыре символа)

2014

9.10.1 Том издания (арабскими цифрами)

не заполнено

9.10.2 Номер издания/Выпуск (арабскими цифрами)

не заполнено

9.11 Страницы (для статей и тезисов - через дефис, без пробела и без меток «с.», «стр», «рр.», «р» и т.п.; для монографий – только общее количество страниц)

131

9.12.1 Полное название издательства (указывается на языке оригинала; для монографий, статей в сборнике, статей в продолжающихся изданиях – обязательно)

СПОИСУ. – СПб

9.12.2 Город, где расположено издательство

Санкт-Петербург

9.13 Краткий реферат публикации (не более 1 страницы; для всех публикаций, в том числе для публикаций в зарубежных изданиях, реферат – только на русском языке)

В работе предлагается концептуальная модель системы защиты встроенных устройств, определяющая процесс комбинирования отдельных компонентов защиты, реализующих различные свойства безопасности устройства путем выбора эффективных компонентов с учетом их нефункциональных свойств и ограничений устройства.

Модель описывает действия, которые должен выполнить разработчик встроенного устройства при конфигурировании его компонентов защиты. Применение существующих нормативов и стандартов позволяет среди имеющихся базовых компонентов защиты выбрать те из них, которые отвечают требованиям стойкости и надежности в соответствии с моделью нарушителя и актуальными видами угроз встроенного устройства.

9.14 Общее число ссылок в списке использованной литературы (цифрами)

не заполнено