УДК 004.056.53

И.В. Котенко, И.Б. Саенко

ПОСТРОЕНИЕ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИСОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ КИБЕРНЕТИЧЕСКОГО ПРОТИВОБОРСТВА

Котенко И.В., Саенко И.Б. **Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства.**
Аннотация. Кибернетическое противоборство знаменует собой новый уровень информационного противоборства, имеющего место в компьютерной инфраструктуре. Новым и достаточно перспективным направлением в защите информации в условиях киберпротивоборства является построение системы интеллектуальных сервисов защиты информации. Система интеллектуальных сервисов защиты информации использует технологию управления информацией и событиями безопасности, что позволяет ей успешно противостоять кибератакам и кибертерроризму и обеспечивать необходимый уровень кибербезопасности защищаемой инфраструктуры. В статье рассматриваются основные положения по построению системы интеллектуальных сервисов защиты и ее отдельных компонентов. На основании результатов рассмотрения общих положений по построению системы интеллектуальных сервисов защиты информации представлены подходы к реализации ряда базовых интеллектуальных сервисов защиты, таких как сервисы сбора, преобразования и хранения информации о событиях безопасности, сервисы моделирования атак и поведения защищаемой системы, сервисы поддержки принятия решений в области обеспечения безопасности и сервисы визуализации информации о безопасности.
Ключевые слова: информационная безопасность, сервисы защиты информации, события безопасности, интеллектуализация защиты, моделирование сетевых атак, репозиторий, визуализация.

Kotenko I.V., Saenko I.B. **Developing the system of intelligent services to protect information in cyber warfare.**
Abstract. Cyber warfare marks a new level of information confrontation occurring in computer infrastructure. New and very promising area of information security in conditions of cyber warfare is to build the system of intelligent information protection services. The system of intelligent information protection services uses the technology of security information and event management, which enables to withstand cyber-attacks and cyber terrorism and to ensure the necessary level of infrastructure cyber security. The paper discusses the basic issues for development a system of intelligent protection services and its individual components. Based on the analysis of general regulations for realizing a system of intelligent information protection services, the paper provides a number of basic approaches for implementation intelligent services, such as services for collecting, converting and storing information about security events, services for modeling of attacks and protection system behavior, security decision support services and information visualization services.
Keywords: information security, information protection services, security event, intellectualization of protection, network attack modeling, repository, visualization.

1. Введение. Информационное противоборство в компьютерной инфраструктуре, иначе называемое *кибернетическим противоборством* или *киберпротивоборством*, занимает одно из центральных

мест в деятельности не только политических и государственно-административных, но также промышленно-экономических, силовых, научно-технических, образовательных и прочих структурах и организациях.

Отличительными чертами киберпротивоборства являются низкая предсказуемость места возникновения, направленности и способа реализации информационного воздействия (программных атак) на ресурсы защищаемой компьютерной инфраструктуры, а также сложность анализа и оценки последствий такого воздействия. Кроме того, воздействие оказывается не только на обрабатываемую информацию и средства ее обработки (как в информационном противоборстве), но также на кадровое и организационное обеспечение инфраструктуры [1].

Несмотря на достаточно большое внимание, уделяемое научными исследованиями ведущих стран тематике киберпротивоборства и кибербезопасности, говорить о наличии удовлетворительного решения данной проблемы преждевременно. Одной из причин такого положения дел является то, что применение традиционных средств и систем защиты информации в интересах обеспечения кибербезопасности в силу специфики угроз, характерных для киберпротивоборства, является недостаточным.

Одним из актуальных направлений обеспечения кибербезопасности является *интеллектуализация сервисов защиты* информации, которая предполагает широкое внедрение в систему защиты интеллектуальных средств, моделей и методов, или *интеллектуальных сервисов*. В первую очередь интеллектуальные сервисы осуществляют интегральную оценку состояния сети, управление безопасностью и адаптацию политик безопасности и компонентов системы защиты информации. В этом случае *система интеллектуальных сервисов защиты информации* (СИСЗИ) является тем необходимым средством, которое позволяет успешно противостоять кибератакам и кибертерроризму и обеспечивать необходимый уровень кибербезопасности защищаемой инфраструктуры в условиях киберпротивоборства.

Целью статьи является рассмотрение основных вопросов, связанных с построением СИСЗИ как специфической для обеспечения кибербезопасности системы. На основании результатов рассмотрения понятия СИСЗИ представлены предложения по реализации ряда интеллектуальных сервисов защиты информации, которые в СИСЗИ, по нашему мнению, являются базовыми.

2. Понятие системы интеллектуальных сервисов защиты информации. Реализация принципов, методов, моделей и алгоритмов

интеллектуализации защиты информации в компьютерной инфраструктуре переводит традиционную систему защиты информации (СЗИ) на новый уровень, наделяя ее качественно новыми функциональными возможностями, необходимыми для решения задач обеспечения кибербезопасности. В результате можно говорить не о традиционной, а об *интеллектуальной системе защиты информации* (ИСЗИ).

Раскроем терминологический аппарат, который связан с новыми подсистемами, образующими ИСЗИ наравне с традиционной СЗИ.

Для подсистемы ИСЗИ, которая непосредственно осуществляет перевод традиционной СЗИ на интеллектуальный уровень, применяется термин «система интеллектуализации защиты информации» (СИЗИ). Тем самым подчеркивается значение понятия «интеллектуализации» как процесса, осуществляющего наращивание возможностей традиционной СЗИ за счет внедрения в эту систему интеллектуальных сервисов защиты. СИЗИ следует воспринимать как интеллектуальную надстройку над традиционной СЗИ, которая не подменяет, а дополняет функциональные возможности последней.

В то же время следует отметить, что СИЗИ является системой с управлением. Объектами управления в ней выступают отдельные *интеллектуальные сервисы защиты*. Управление ими осуществляет *система* (подсистема) *управления интеллектуальными сервисами защиты информации*. В результате для СИЗИ, как для системы с управлением, на наш взгляд, вполне пригодным является и другой термин, который уже был упомянут выше, а именно *система интеллектуальных сервисов защиты информации*.

Объекты и субъекты защиты для СИСЗИ остаются такими же, как в традиционной системе защиты. Объектами защиты являются информационные и телекоммуникационные ресурсы компьютерной инфраструктуры, а субъектами защиты, т.е. лицами, осуществляющими управление безопасностью информации, являются администраторы безопасности.

Выработка решений по защите информации осуществляется путем обработки информации о *событиях кибербезопасности*. К информации такого рода относятся все данные об изменении состояния элементов защищаемой компьютерной инфраструктуры, формируемые программным или аппаратным способом, подлежащие хранению в электронном виде в специальных журналах в форме учетных записей (логов) или поступающие непосредственно в модуль анализа и сбора информации по каналам связи. Помимо этого, к событиям кибербезопасности следует отнести события, приводящие к критическому из-

менению бизнес-процессов, а также параметров физических датчиков информации, задействованных в защищаемой инфраструктуре.

В качестве источников информации о событиях кибербезопасности выступают элементы защищаемой компьютерной инфраструктуры различных типов и производителей: серверы баз данных, серверы компьютерной сети, рабочие станции, межсетевые экраны, системы обнаружения атак, антивирусы, виртуальные сети, управляемые сетевые маршрутизаторы (коммутаторы) и другие средства. Помимо них, источниками являются прикладные приложения бизнес-процессов и физические датчики, контролирующие параметры защищаемой инфраструктуры.

Так как сбор, хранение и обработка данных о событиях кибербезопасности (далее – событиях безопасности) лежат в основе функционирования СИСЗИ, представляется целесообразным использовать для ее построения идеологию «системы управления информацией и событиями безопасности» (Security Information and Event Management System, SEIM) [2, 3]. В общих чертах особенности построения такого класса систем заключаются в следующем.

Информация, содержащаяся в указанных источниках, подлежит сбору и последующей обработке в СИСЗИ. Результатом этой обработки является выработка предупреждений или непосредственных решений по перенастройке или реконфигурации традиционных средств защиты.

Типовой тракт обработки этой информации в СИСЗИ составляют следующие процессы: сбор информации о событиях безопасности; приведение информации безопасности к единому внутреннему формату представления; хранение событий безопасности в информационном хранилище; выдача необходимых данных из хранилища по запросам аналитических модулей; анализ данных, полученных по запросам, в аналитических модулях и модулях моделирования для принятия решений; визуализация событий безопасности и управленческих решений и формирование по ним отчетности.

В соответствии с данным трактом обработки информации о событиях безопасности в СИСЗИ следует выделять три уровня, или слоя, элементов: сбора и преобразования формата представления исходной информации; хранения, поиска и выдачи информации по запросам аналитических модулей либо субъектов защиты; анализа информации и выработки решений.

На первом уровне реализация соответствующих функций возлагается на сервисы, связанные с преобразованием информации во внутренний формат хранения и использования.

На втором уровне используются программно-инструментальные средства хранения данных. В настоящее время наиболее популярными являются реляционные и XML-ориентированные системы управления базами данных (СУБД).

На третьем уровне выполняется интеллектуальный анализ данных, полученных по запросам из информационного хранилища. Данный анализ включает корреляцию событий безопасности, моделирование и прогнозирование атак и поведения системы, выработку предупреждений и управленческих решений, формирование отчетности и визуализацию текущих и итоговых данных.

Следовательно, можно отнести к числу базовых интеллектуальных сервисов, определяющих специфику СИСЗИ как интеллектуальной системы, следующие компоненты: сбор, преобразование и хранение информации о событиях безопасности; моделирование атак и поведение защищаемой системы; поддержка принятия решений в области обеспечения безопасности; визуализация информации.

Рассмотрим подходы, предлагаемые для реализации указанных выше сервисов.

3. Сервисы сбора, преобразования и хранения информации о событиях безопасности. Интеллектуальные сервисы сбора, преобразования и хранения информации о событиях безопасности являются важнейшими компонентами СИСЗИ. Основными функциями, которые реализуют данные сервисы, являются преобразование входных данных во внутренний универсальный формат, их корреляция и хранение в репозитории.

Сервисы сбора данных о событиях должны поддерживать различные протоколы взаимодействия и иметь возможность настройки новых протоколов и входных форматов. Наиболее популярными протоколами передачи журнальных данных являются Syslog, FTP, ODBC и SNMP. Кроме того, важно не только поддерживать транспортный протокол, но и распознавать формат и семантику содержимого журнала. Для этих целей имеются форматы Syslog, CLF, SCAP, CIM и CEF, предлагаемые для его использования различными поставщиками продуктов в области безопасности.

Однако в целях построения СИСЗИ и в связи с развитием средств интеллектуального анализа данных такие простые форматы не могут удовлетворять следующим требованиям: поддержка структурирован-

ного представления информации; использование меток времени; обеспечение иерархической структуры для представления информации.

В настоящий момент нет универсального решения относительно формата, удовлетворяющего данным требованиям. Поэтому необходимо обоснование подхода к построению такого формата, способного применяться в различных прикладных областях и быть достаточно выразительным и расширяемым.

На наш взгляд, наиболее перспективным представляется *онтологический подход* к представлению данных [4]. Данный подход предполагает использование специального формализованного описания предметной области, основанного, как правило, на дескрипционной логике, получившей название *онтологии*. Суть онтологического подхода заключается в том, что вначале выделяется набор концептов (базовых понятий данной предметной области). Затем строятся связи между концептами, т.е. задаются отношения между базовыми понятиями. В простейшем случае онтология описывает только иерархию концептов-отношений, связанных отношениями категоризации.

По сути онтологии играют роль баз знаний и обладают всеми преимуществами последних. В частности, онтологическая архитектура имеет слабосвязанное, модульное представление, устойчивое к быстрым изменениям и сложности. Основанные на такой архитектуре сервисы и приложения могут свободно объединять и расширять архитектурные компоненты во время своего выполнения в интересах контекста приложения. Данное обстоятельство весьма уместно для СИСЗИ, так как этой системе необходима наиболее общая и неперегруженная модель данных, которая в то же время адаптирована и конкретизирована для различных областей применения.

Следует отметить, что при онтологическом подходе изменение модели данных требует значительно меньших усилий, чем в реляционных моделях. Кроме того, математический аппарат, положенный в основу онтологического подхода, позволяет строить более точные запросы на выборку и, тем самым, значительно уменьшать время, затрачиваемое аналитическими модулями на выборку информации из хранилища для ее последующего анализа.

Следующий этап обработки данных о событиях безопасности — *корреляция* событий, под которой понимается сопоставление различной информации об одинаковых событиях или явлениях, полученных от различных источников, с целью устранения имеющейся в них неопределенности и/или получения новой достоверной информации о безопасности. Процесс корреляции информации тесно связан с про-

цессом получения новой информации на основе анализа хранимых онтологий в условиях их неполноты и противоречивости.

Данные о событиях безопасности, прошедшие все вышеописанные процедуры обработки, помещаются в репозиторий. В качестве базовой архитектуры репозитория целесообразно использовать архитектуру SOA (архитектуру, ориентированную на сервисы), которая реализуется как набор web-сервисов, используемых для доступа к данным в репозитории.

Наиболее распространенным решением для построения репозитория на настоящий момент являются реляционные СУБД. Модель данных в реляционной СУБД можно представить диаграммой «сущность-связь». Репозиторий на основе XML-СУБД представляется в виде древовидно-организованной файловой системы. Модель данных описывается с помощью XML-схемы. Триплет является тройкой «субъект» — «предикат» — «объект». Хранилище триплетов обеспечивает большую гибкость изменения модели данных, однако оно проигрывает реляционной СУБД по производительности.

Учитывая достоинства и недостатки перечисленных выше средств создания репозитория, представляется целесообразным использовать гибридное решение, поддерживающее все эти три вида хранилищ [5]. Примером такого средства является система Virtuoso Universal Server компании OpenLink [6].

Онтологический подход к построению сервисов сбора, преобразования и хранения информации позволяет реализовать в СИСЗИ системы логического вывода, основанные на онтологии. Так, в настоящее время для этой цели получает широкое распространение язык OWL (Web Ontology Language). Кроме OWL для логического вывода используется SWRL (Semantic Web Rule Language).

4. Сервисы моделирования атак и поведения защищаемой системы. Предлагаемый подход к построению сервисов моделирования атак и поведения защищаемой системы предполагает: моделирование объекта защиты и поведения злоумышленника; генерацию общего графа атак; вычисление различных показателей безопасности; предоставление всеобъемлющих процедур анализа риска.

Для моделирования атак в компьютерных системах существует множество подходов. Для СИСЗИ, на наш взгляд, в первую очередь заслуживает внимание подход, использующий таксономии. В частности, известны следующие таксономии атак: списки элементов атак, списки классов атак, классы результатов атак, практические списки типов атак, матрицы уязвимостей, таксономии дефектов безопасности

или уязвимостей, таксономии инцидентов и другие. Примером таксономии событий является общий язык для описания инцидентов безопасности [7], в котором три основных понятия языка («инцидент», «атака» и «событие») определяются следующими группами вспомогательных понятий: «атакующие», «продукты», «уязвимости», «действия», «мишени», «нелегитимные результаты» и «цели».

Атака рассматривается как упорядоченные по времени действия, включающие некоторое исходное действие нарушителя, за которым следуют вспомогательные действия, и т.п. В эту модель также могут быть включены ответные и другие действия, инициируемые сотрудником службы безопасности, обычными пользователями, другими нарушителями и т.д. Итоговая последовательность действий моделирует использование уязвимостей для осуществления нелегитимной угрозы безопасности [8, 9].

Общая концепция атаки рассматривает атаку как комплекс действий, состоящий из трех фаз: «сбора информации», «эксплуатации» и «метастазы». Последняя может быть логически разделена на подфазы «закрепление» и «развитие» [10]. В процессе закрепления скрывается очевидность проникновения на хост, расширяются привилегии, и подготавливается удаленный нелегитимный доступ. На подфазе развития злоумышленник пытается проникнуть глубже на другие хосты.

Обычно смоделированные атаки представляются в виде графов (*графов атак*). Узлы графов атак раскладываются на И-декомпозицию (набор подцелей, каждая из которых должна быть достигнута для успеха атаки) или на ИЛИ-декомпозицию (набор подцелей, достижение одной из которых достаточно для успеха атаки) [11].

Таким образом, математическая модель целей атаки определяется в виде $MA = \langle \{G_i\}, \{S_u\} \rangle$, где $\{G_i\}$ — формальные грамматики, $\{S_u\}$ — операции «замещения». Каждая формальная грамматика определяется пятеркой $G = \langle VN, VT, S, P, A \rangle$, где G — имя грамматики, VN — набор нетерминальных символов (которые относятся к верхнему и среднему уровням сценария атаки), VT — набор терминальных символов, которые обозначают действия злоумышленника, отображенные как шаги низкоуровневого сценария атаки, P — набор продуктов, которые определяют специальные операции для цели через замещение символов узла верхнего уровня символами узлов нижнего уровня, и A — набор атрибутов и алгоритмов их вычисления.

Каждый продукт образуется как $\left[\left(U\right)\right] X \to \alpha\left(Prob\right)$, где U — условие для использования правила, [ ] — обозначает, что элемент в скобках необязательный, X — нетерминальный символ, α — строка терминальных и нетерминальных символов, $Prob$ — исходное значение вероятности правила, выбранного для заданной цели.

Алгоритмическое отображение генерации атаки, определенное как семейство формальных универсальных грамматик, может быть реализовано семейством машин состояний. Базовые элементы каждой машины состояний — состояния, дуги переходов, объяснительный текст для каждого перехода. Состояния каждой машины состояний разделены на три типа: первый (исходный), средний, и итоговый. Исходное и среднее состояния следующие: нетерминальное, такое, что инициирует работу соответствующих вложенных машин состояний; терминальное, такое, что взаимодействует с моделью хоста; абстрактные (дополнительные) состояния.

Дуги переходов определяются правилами грамматик и могут быть выполнены только при определенных условиях. Внутри состояния, за исключением выбора перехода, зависящего от цели и текущей вероятности перехода, могут быть предприняты следующие типы действий: *входное* (действие, предпринятое при входе в состояние); *активное* (набор базовых действий, включающих действия перехода на вложенную машину состояний или реализацию модели реакции хоста); *выхода* (действие, предпринимаемое для выхода).

Модель каждой машины состояний устанавливается определением следующих компонент: диаграмма машины состояний; основные параметры машины состояний; параметры переходов, которые определяют стохастическую модель функционирования машины состояний для различных подходящих целей соответственно реализации сетевых атак; условия переходов. Основные параметры машины состояний включают имя машины состояний, соответствующие цели, состояния, первое состояние, нетерминальное, терминальное и дополнительные состояния [12–14].

5. Сервисы поддержки принятия решений в области обеспечения безопасности. Для построения сервисов поддержки принятия решений в СИСЗИ может быть использовано несколько методологических подходов.

В [15] выделены фильтрующие методы, группирующие методы и процедуры, основанные на поиске.

Первый класс подходов уменьшает набор эффективных вариантов выбора, отбрасывая наиболее «избыточные» точки, удерживая решения, наиболее непохожие. Пример применения подхода такого класса в контексте выбора защитных средств информационной безопасности дан в [16], где используется структура данных «k-дерево» [17].

Группирующие методы могут быть применены к формированию групп одинаковых вариантов. Если задано управляемое количество кластеров, то администратору безопасности дается представляющая точка от каждого кластера. Администратор может выбрать наиболее предпочтительное из этих решений и проверить окрестности этой точки. Для этой цели можно использовать неиерархическую группировку «k-средних» [18].

Процедуры, основанные на поиске, начинаются с эффективного выбора и позволяют лицу, принимающему решения, «двигаться» в пространстве решений к более привлекательным альтернативам до того, как найдено «наилучшее» решение [19].

Кроме того, для задачи защиты компьютерной инфраструктуры целесообразен интерактивный подход к поддержке решений, основанный на поиске [20], который уже применялся в похожем контексте в [21]. Следуя этому подходу, администратор безопасности итеративно создает желаемые уровни для целей или изменяет верхние и нижние границы через графический интерфейс и, таким образом, снижает набор вариантов-кандидатов. Достоинство подхода лежит не только в производимом выборе, но и в понимании, которое администраторы безопасности получают на каждом уточняющем шаге оценки.

6. Сервисы визуализации информации о событиях безопасности. В отличие от обработки текстовых данных визуализация предлагает более эффективный подход к анализу информации. *Визуализация информации* в СИСЗИ представляет собой процесс генерирования изображения на основе событий безопасности и результатов функционирования сервисов защиты [22]. С помощью визуализации данных можно обобщать множество отдельных деталей таким образом, чтобы сделать доступным смысл того или иного события и совокупности событий. Визуализация также позволяет, используя различные формы, цвета, размеры и взаимное расположение элементов, повысить оперативность восприятия больших объемов воспринимаемой информации.

Известны следующие классы графов, которые можно использовать для построения сервисов визуализации информации в СИСЗИ [23]: простые диаграммы; диаграммы с накоплением; схемы полигонов; диаграммы рассеивания; графы параллельных координат;

графы связей; карты; карты деревьев. Каждый из этих графов имеет разные возможности и подчеркивает конкретные аспекты данных. Наиболее специфичными, на наш взгляд, являются схемы полигонов и графы параллельных координат.

Схема полигонов предназначена для показа распределения значений. Примером является распределение размера пакетов по протоколам (рис. 1). Данная схема имеет два измерения, причем категориальные измерения могут быть использованы для разбиения графика на несколько участков для сравнения.

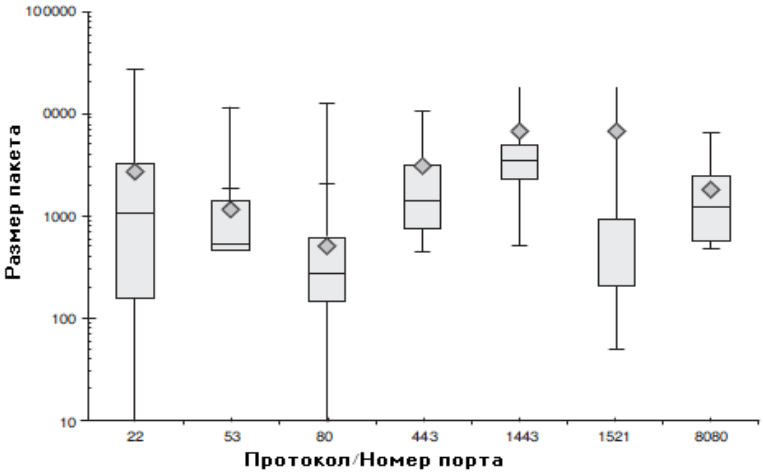

Рис. 1. Пример распределения размера пакетов по протоколам.

Граф параллельных координат используется для представления многомерных данных в одной плоскости. Примером является анализ наборов правил межсетевого экрана с показом для каждого правила объема связанного с ним трафика (рис. 2).

Процесс поиска наилучшего способа визуализации данных согласно [24] имеет следующие этапы: обзор; масштабирование; фильтрация; детализация. Формализация процесса визуализации, предложенная Ю.В. Энгельгардтом и К.С. Дурстелером, включает шесть основных шагов: фильтрация; нормализация; визуальная трансформация; преобразование представления; интерпретация и принятие решения.

Как правило, выделяются три основные категории назначения визуализации: для отчетности; для проведения исторического анализа данных; для мониторинга в реальном времени.

Предлагаемая архитектура компонента, реализующего сервисы визуализации, строится на основе трехуровневой модели, включающей пользовательский интерфейс, управляющие сервисы, состоящие из контроллера графических элементов и менеджера сервисов, осуществляющих управление низкоуровневыми элементами модели графическими элементами и другими сервисами [25]. Выделение пользовательского интерфейса в отдельный уровень позволяет поддерживать разработку различных видов пользовательских форм, начиная от простой командной строки, заканчивая сложным многооконным интерфейсом с различными панелями управления. Контроллер графических компонентов предоставляет стандартный интерфейс по работе с потоками визуализации, поступающими от пользовательского интерфейса или от других сервисов. Менеджер сервисов компонентов обеспечивает подключение сервисов. Уровень графических элементов представляет собой библиотеку необходимых графических примитивов, таких как графы, лепестковые диаграммы, гистограммы, карты деревьев (плоские деревья), географические карты и т.д. Они реализуют обработку входных данных, их отображение и взаимодействие пользователя непосредственно с входными данными.

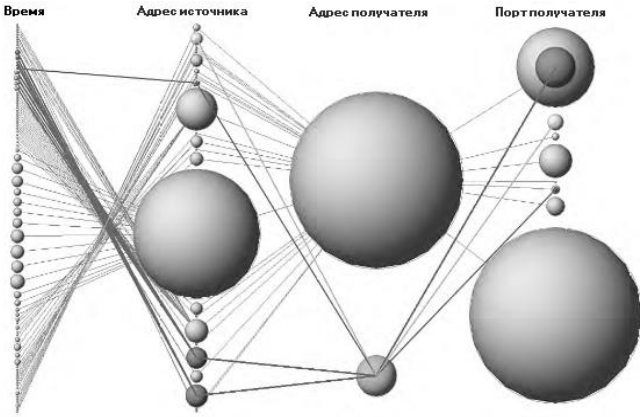

Рис. 2. Пример визуализации данных анализа правил межсетевого экрана.

7. Заключение. Таким образом, в статье рассмотрены подходы к построению базовых компонентов СИСЗИ в условиях киберпротивоборства. Предложенная архитектура СИСЗИ отличается тем, что рассматривается как интеллектуальная надстройка над традиционной системой защиты информации.

Отличительной особенностью рассмотренных интеллектуальных сервисов защиты является их инвариантность относительно существующих и разрабатываемых типов программных атак, а также способность вырабатывать предупреждения и управляющие решения по безопасности информации в реальном или близком к реальному масштабу времени.

Полученные результаты по построению и использованию СИСЗИ целесообразно использовать для разработки методов, моделей и алгоритмов анализа защищенности, оценки рисков и верификации политики безопасности, использования репозитория и механизмов логического вывода, а также моделей поддержки принятия решений по защите информации и визуализации, ориентированных на применение для защиты информации в критически важных компьютерных инфраструктурах.

Литература

1. Понимание киберпреступности. Руководство для развивающихся стран. Отчет МСЭ. 2009. 226 с. http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
2. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012.
3. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012.
4. *Kotenko I., Polubelova O., Saenko I.* Data Repository for Security Information and Event Management in Service Infrastructures // SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24–27 July 2012.
5. *Kotenko I., Polubelova O., Saenko I.* Hybrid Data Repository Development and Implementation for Security Information and Event Management // Proc. of the Work in Progress Session 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February 2012.
6. Virtuoso Universal Server. http://virtuoso.openlinksw.com.
7. *Howard J.D., Longstaff T.A.* A Common Language for Computer Security Incidents. SANDIA REPORT, SAND98–8667, 1998.
8. *Amoroso E.G.* Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion. Net Book, 1999.
9. *Amoroso E.* Cyber Attacks: Protecting National Infrastructure. Butterworth-Heinemann, 2011.
10. *Cheswick W.R., Bellovin S.M.* Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Publishing Company, Reading, MA, 1994.
11. *Moore A.P., Ellison R.J., Linger R.C.* Attack Modeling for Information Security and Survivability // Technical Note CMU/SEI–2001–TN–001. Survivable Systems, 2001.
12. *Gorodetski V., Kotenko I.* Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool // Lecture Notes in Computer Science, Vol.2516, 2002.

13. *Kotenko I.* Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks // Lecture Notes in Artificial Intelligence, Springer Verlag. Vol. 2691, 2003. Pp.464–474.
14. *Kotenko I., Mankov E.* Agent-Based Modeling and Simulation of Computer Network Attacks // Fourth International Workshop «Agent-Based Simulation 4 (ABS 4)». Proceedings. Montpellier, France, 2003.
15. *Graves S.B., Ringuest J.L.* Models & Methods for Project Selection, Berlin/Heidelberg: Springer, 2002.
16. *Strauss C., Stummer C.* Multiobjective decision support in IT-risk management // International Journal of Information Technology & Decision Making, vol. 1, no. 2, 2002. P. 251–268.
17. *Sun M., Steuer R.E.* InterQuad: An interactive quad tree based procedure for solving the discrete alternative multiple criteria problem // European Journal of Operational Research, vol. 89, no. 3, 1996. P.462–472.
18. *Jobson J.D.* Applied Multivariate Data Analysis: Volume II: Categorical and multivariate methods, Berlin/Heidelberg: Springer, 1992. 731 p.
19. *Stummer C., Kiesling E., Gutjahr W.J.* A multicriteria decision support system for competence-driven project portfolio selection // International Journal of Information Technology & Decision Making, vol. 8, no. 2, 2009. P.379–401.
20. *Stummer C.* Projektauswahl im betrieblichen F&E-Management, Wiesbaden: Gabler, 1998.
21. *Wojcik M.N.* Proposed Remediation Specifications. http://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_DoD_Wojcik.pdf.
22. *Marty R.* Applied security visualization. New York: Addison-Wesley Professional, 2008.
23. *Ma K.-L.* Cyber Security Through Visualization // Asia Pacific Symposium on Information Visualization (APVIS 2006), Vol. 60. Tokyo, Japan. 2006.
24. *Card S. K., Mackinlay J., Shneiderman B.* Readings in Information Visualization: Using Vision to Think (Interactive Technologies). Morgan Kaufmann, 1999.
25. Новикова Е.С. Механизмы визуализации в SIEM-системах // Четырнадцатая Международная конференция “РусКрипто’2012”. Московская область, Солнечногорск, 28–30 марта 2012 г. http://www.ruscrypto.ru

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Professor, Head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — more than 450. ivkote@comsec.spb.ru,

www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Саенко Игорь Борисович — д–р техн.наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность, теория моделирования, теория информации. Число научных публикаций — более 250. ibsaen@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of Laboratory of Computer Security Problems, SPIIRAS. Research interests: automated information systems, information security, theory of modeling, information theory. The number of publications — more than 250. ibsaen@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ (проекты 10–01–00826–а, 11–07–00435–а), программой фундаментальных исследований ОНИТ РАН ((проект 2.2) и проектами Седьмой рамочной программы Европейского Союза *SecFutur* и *MASSIF*.

Рекомендовано лабораторией криптологии, заведующий лабораторией Молдовян Н.А., д–р техн.наук, проф., заслуженный изобретатель РФ.
Статья поступила в редакцию 31.05.2012.

РЕФЕРАТ

Котенко И.В., Саенко И.Б. **Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства.**

Кибернетическое противоборство знаменует собой новый уровень информационного противоборства, имеющего место в компьютерной инфраструктуре. Новым и достаточно перспективным направлением в защите информации в условиях киберпротивоборства является построение системы интеллектуальных сервисов защиты информации. Система интеллектуальных сервисов защиты информации использует технологию управления информацией и событиями безопасности, что позволяет ей успешно противостоять кибератакам и кибертерроризму и обеспечивать необходимый уровень кибербезопасности защищаемой инфраструктуры. В статье рассматриваются основные положения по построению системы интеллектуальных сервисов защиты и ее отдельных компонентов. На основании результатов рассмотрения общих положений по построению системы интеллектуальных сервисов защиты информации представлены подходы к реализации ряда базовых интеллектуальных сервисов защиты, таких как сервисы сбора, преобразования и хранения информации о событиях безопасности, сервисы моделирования атак и поведения защищаемой системы, сервисы поддержки принятия решений в области обеспечения безопасности и визуализации информации о безопасности.

Для сервисов сбора, преобразования и хранения информации о событиях безопасности предложен онтологический подход, согласно которому внутреннее представление информации предлагается осуществлять с использованием онтологий различных предметных областей. Для реализации репозитория, в котором хранятся данные о событиях безопасности, выдаваемые по запросам аналитических модулей, предлагается гибридный подход, сочетающий в себе возможности реляционных СУБД, XML-ориентированных СУБД и хранилища триплетов.

Для сервисов моделирования атак и поведения защищаемой системы предлагается реализация таких возможностей как моделирование объекта защиты и поведения злоумышленника, генерация общего графа атак, вычисление различных показателей безопасности, предоставление всеобъемлющих процедур анализа риска.

Для сервисов поддержки принятия решений в области обеспечения безопасности предлагается использовать фильтрующие методы, группирующие методы и процедуры, основанные на поиске. Кроме того, для задачи защиты компьютерной инфраструктуры целесообразен интерактивный подход к поддержке решений, основанный на поиске.

Для сервисов визуализации информации о безопасности предлагается использовать все известные классы графов. Визуализация данных позволяет, используя различные формы, цвета, размеры и взаимное расположение элементов, повысить оперативность восприятия больших объемов информации.

SUMMARY

Kotenko I.V., Saenko I.B. **Developing the system of intelligent services to protect information in cyber warfare.**

Cyber warfare marks a new level of information confrontation occurring in computer infrastructure. New and very promising area of information security in conditions of cyber warfare is to build the system of intelligent information protection services. The system of intelligent information protection services uses the technology of security information and event management, which enables to withstand cyber-attacks and cyber terrorism and to ensure the necessary level of infrastructure cyber security. The paper discusses the basic issues for developing a system of intelligent protection services and its individual components. Based on the analysis of general regulations for realizing a system of intelligent information protection services, the paper provides a number of basic approaches for implementation intelligent services, such as services for collecting, converting and storing information about security events, services for modeling of attacks and protection system behavior, security decision support services and information visualization services.

For services intended to collect, transform, and store security event information we offer the onthological approach. According to this approach, the internal representation of information should be carried out with the use of onthologies of various subject areas. To implement a repository that stores security event data, issued at the requests of analytical modules, a hybrid approach is suggested. This approach combines the capabilities of relational database systems, XML- databases and storage of triplets.

For services intended to model the attack and the protected system behavior, we suggest to realize such features as modeling of protection object or attacker's behavior, generation of the overall attack graph, calculation of different security metrics, provision of comprehensive risk analysis procedures.

For security decision support services, we suggest to use the filtering methods, grouping methods and search-based procedures. In addition, for computer infrastructure protection a search-based interactive approach for supporting solutions is appropriate.

For security information visualization services, all known classes of graphs are proposed to be implemented. Data visualization allows the increasing the efficiency of perception of large amounts of information by means of different shapes, colors, sizes and positioning of elements.