А. Н. Шниперов, Е. А. Сантьев,
Институт космических и информационных технологий Сибирского федерального университета, г. Красноярск

ПОДХОДЫ К ПРОЕКТИРОВАНИЮ ЗАЩИЩЕННЫХ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ

Аннотация
Обеспечение безопасности гетерогенных информационных систем в силу их сложной архитектуры предполагает использование новых подходов к проектированию систем защиты. В статье приводятся общие положения по построению и функционированию нового перспективного класса интеллектуальных систем защиты информации, базирующихся на концепции управления информацией и событиями безопасности (SIEM).
Ключевые слова: информационная безопасность, SIEM, интеллектуальные системы защиты информации, события безопасности.

Современные тенденции применения информационных технологий в образовании, особенно профессиональном, во многом связаны с созданием образовательных порталов, где не только сосредоточены и упорядочены информационные ресурсы, но и строятся индивидуальные траектории обучения, применяются различные способы донесения материала до обучаемого, внедряются интерактивные элементы и т. д. Такие образовательные порталы предоставляют и развитые средства коммуникации между участниками: чаты, форумы, вебинары, видеоконсультации и т. д. В настоящее время в мире существует достаточно большое количество подобных порталов, реализующих различные педагогические подходы к обучению, например: Coursera (https://www.coursera.org), академия Хана (https://www.khanacademy.org), образовательный портал UniverTV (http://univertv.ru) и др. Их объединяет сам подход к созданию современной информационно-образовательной среды — в виде портала.

С технической точки зрения такого рода *информационно-образовательные системы (ИОС)* представляют собой консолидацию различных технологических решений, позволяющих воплотить в жизнь необходимый инструментарий пользователя (преподавателя, обучаемого и др.). Поэтому разработка, запуск в эксплуатацию и поддержание в рабочем состоянии образовательного портала (с быстрым временем реакции) определенно не является тривиальной задачей. С одной стороны, существенное увеличение количества одновременных соединений, а также стремительный рост трафика в информационных системах приводят к необходимости балансирования нагрузок, причем преимущественно за счет создания сложных распределенных систем. С другой стороны, тенденция к созданию интеллектуальных гетерогенных информационных систем требует новых подходов к проектированию и технологической реализации, например, мультиагентного подхода.

Кроме того, внедрение информационно-образовательных технологий в реальный учебный процесс сопровождается накоплением в информационных системах конфиденциальной информации, утечка или компрометация которой может повлечь за собой вполне серьезные издержки. Отказоустойчивость образовательных порталов в учебных учреждениях также должна быть очень высокой, в силу того что сам образовательный процесс уже может базироваться на внедренных информационно-образовательных технологиях [7, ст. 16]. В связи с этим задача обеспечения информационной безопасности информационно-образовательной системы является крайне важной. Причем решать эту задачу необходимо на ос-

Контактная информация

Шниперов Алексей Николаевич, канд. тех. наук, доцент кафедры прикладной математики и компьютерной безопасности Института космических и информационных технологий Сибирского федерального университета, г. Красноярск; *адрес:* 660074, г. Красноярск, ул. Киренского, д. 26, корпус УЛК; *телефон:* (391) 291-27-11; *e-mail:* Ashniperov@sfu-kras.ru

A. N. Shniperov, E. A. Santyev,
Institute of Space and Information Technologies, Siberian Federal University, Krasnoyarsk

APPROACHES TO THE DESIGN OF THE PROTECTED HETEROGENEOUS INFORMATION EDUCATIONAL SYSTEMS

Abstract
Securing heterogeneous information systems, due to their complex architecture involves the use of new approaches to the design of the protection systems. The article describes general provisions on the construction and operation of a new perspective class of intelligent security systems based on the concept of Security Information and Event Management (SIEM).
Keywords: information security, SIEM, intellectual systems of information security, security events.

Рис. 1. Трехзвенная клиент-серверная архитектура

нове внедрения *системы защиты информации (СЗИ)*, проектирование которой должно происходить параллельно с разработкой самой информационно-образовательной системы.

Понятие гетерогенной информационно-образовательной системы

Понятие гетерогенной информационной системы исходит из теории распределенных вычислительных систем, однако оно достаточно широкое и может трактоваться в различных аспектах. *Под гетерогенной информационно-образовательной системой мы будем понимать такую систему образовательной направленности, которая функционирует в рамках парадигмы многозвенной клиент-серверной архитектуры.* В качестве классического примера приведем ее трехзвенный вариант (рис. 1).

Серверная часть системы представляет собой объединение множества узлов (идентичных и разнородных), которые с помощью среды взаимодействия образуют единую информационную среду. Под узлом здесь понимается совокупность технологической платформы, используемого программного обеспечения, технологий обработки и передачи информации. *Клиентская часть* такой системы представляет собой интернет-браузер, реализующий интерфейс пользователя, посредством которого он взаимодействует с информационной средой.

Заметим, что на рисунке 1 представлена упрощенная клиент-серверная архитектура, современные ИОС имеют более сложную организацию, с большим количеством как «вертикальных» уровней распределения серверной части (разнородных узлов), так и «горизонтальных» (однородных узлов). В качестве примера архитектуры гетерогенной ИОС на рисунке 2 представлена общая архитектура информационно-образовательной системы «Курсы СФУ» Сибирского федерального университета (http://ms.sfu-kras.ru), которую в дальнейшем мы будем рассматривать в качестве объекта защиты в вопросах проектирования СЗИ.

Важно отметить, что какой-то универсальной архитектуры реализации гетерогенных ИОС не существует, есть только определенные подходы к проектированию, зависящие от множества различных аспектов. Однако в каждой архитектуре гетерогенной ИОС всегда можно выделить звенья «вертикального» и «горизонтального» распределения (если она проектировалась в рамках распределенной информационно-вычислительной системы с соблюдением необходимых стандартов), что является весомым фактором в вопросах проектирования СЗИ для нее.

Проблемы проектирования СЗИ для гетерогенных информационно-образовательных систем

В гетерогенных системах потенциальное количество угроз в разы выше, чем в «монолитных», а системе защиты информации необходимо противостоять сотням возможных типов атак и их комбинаций, что является первой проблемой проектирования СЗИ. Причин наличия большого количества угроз гетерогенным информационно-образовательным системам много, отметим несколько наиболее весомых:

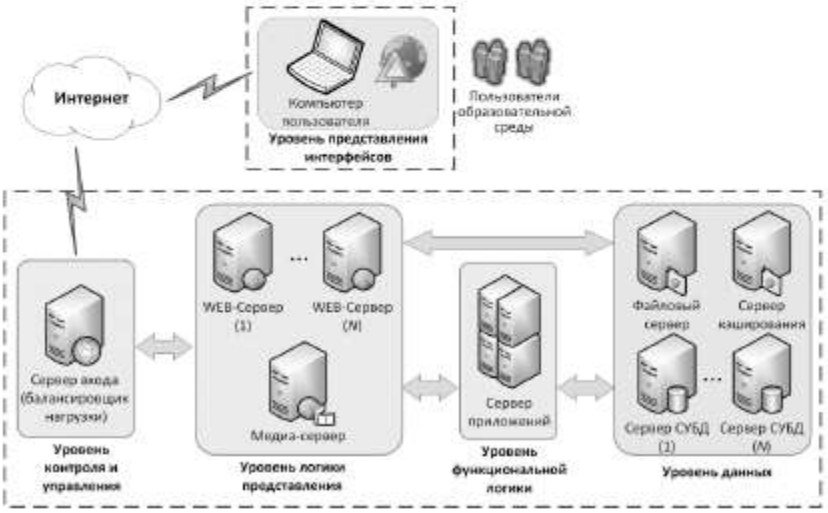

Рис. 2. Общая физическая архитектура гетерогенной информационно-образовательной системы СФУ

- большое количество различных информационных сервисов, представляющих собой функционал ИОС, в каждом из которых априори содержатся алгоритмические и/или технологические ошибки;
- использование сторонних технологических платформ при реализации ИОС (например, если в качестве технологии реализации выбрана платформа Java, то ошибки в самой платформе могут привести к уязвимости ИОС);
- открытый доступ из сети Интернет (соответственно, потенциально возможны самые различные сетевые атаки, например, DDoS-атаки);
- отсутствие целостных стандартов и методик проектирования распределенных ИОС;
- использование сторонних коммерческих компонентов для реализации части функционала ИОС, являющихся закрытыми и безопасность которых трудно или невозможно проверить;
- наличие уязвимостей в системном программном обеспечении;
- использование незащищенных внешних информационных протоколов, потенциальные ошибки в протоколах обмена информацией между различными подсистемами ИОС.

Также необходимо отметить, что разработчики ИОС зачастую серьезно отходят либо вообще не соблюдают эталонную модель среды открытых систем (OSE/RM) [10], которая позволяет еще на этапе проектирования СЗИ определить значимые с точки зрения безопасности характеристики ИОС и ее ключевые компоненты, которые требуют дополнительного внимания со стороны разработчика СЗИ [9].

Однако *самой существенной проблемой проектирования СЗИ является даже не количество угроз, а неопределенность всего их перечня*. Другими словами, количество типов потенциальных угроз — величина недетерминируемая и динамическая, направленная в сторону постоянного увеличения, а значит, предусмотреть алгоритмы выявления всех их еще на стадии проектирования СЗИ попросту невозможно. Поэтому СЗИ должны уметь самостоятельно выявлять новые потенциальные угрозы безопасности ИОС, а также определять и запускать наиболее подходящий механизм защиты. Кроме того, СЗИ должна самостоятельно контролировать эффективность своих решений, чтобы предотвращать серьезные сбои в работе самой ИОС.

Таким образом, сама задача обеспечения информационной безопасности гетерогенных ИОС является интеллектуальный (в рамках классификации, изложенной в [2]), а ее решение требует разработки модели СЗИ с развитыми адаптационными возможностями ее компонентов, в том числе алгоритмов автоматического ситуационного поиска решений.

Подходы к проектированию интеллектуальных СЗИ информационно-образовательной системы

В настоящий момент вопросы, касающиеся проектирования интеллектуальных СЗИ, активно обсуждаются в литературе. Исследователями предлагаются различные инновационные подходы к обнаружениям угроз безопасности, а также механизмы противодействия им. В работах [5, 6, 13] предлагается использование нейронных сетей для выявления атак на информационные системы и предупреждение угроз, в работах [4, 11] авторы строят механизмы защиты на базе концепции иммунных систем, в [1] рассматриваются эволюционные алгоритмы, в [9, 10] нами рассматривается мультиагентный подход к построению интеллектуальных СЗИ.

Кроме того, перспективным направлением создания интеллектуальных СЗИ гетерогенных информационно-образовательных систем является разработка «проактивных» систем безопасности на основе идеологии SIEM (Security Information and Event Management — управление информацией и событиями безопасности). Проактивность СЗИ подразумевает наличие в ней механизмов автоматического выявления потенциальной угрозы безопасности ИОС и принятия мер по ее устранению до того, как ситуация станет критической (произойдет инцидент нарушения безопасности). Для этого СЗИ должна «уметь» анализировать события, происходящие на всех хостах гетерогенной ИОС, вероятностно прогнозировать возможные события и иметь средства управления значимыми (с позиции информационной безопасности) системными и прикладными процессами напрямую и/или посредством конфигурационных файлов.

Системы защиты информации, проектируемые в рамках SIEM-идеологии, должны решать самые разные задачи обеспечения безопасности функционирования информационно-телекоммуникационных инфраструктур и выявлять широкий список угроз [8]. При этом сама SIEM-идеология носит описательный характер общей идеологии, конкретных функциональных и архитектурных моделей либо не существует, либо они носят частный характер и адаптированы для конкретных информационно-коммуникационных инфраструктур.

Тем не менее разработка СЗИ, базирующейся на принципах SIEM-идеологии, является перспективным направлением [12], о чем свидетельствует и развитие проекта по созданию перспективных систем управления информацией и событиями безопасности MASSIF (MAnagement of Security information and events in Service Infrastructures), поддерживаемого Седьмой рамочной программой Европейского союза (FP7-ICT-2009-5).

SIEM-идеологию можно весьма эффективно использовать в качестве базиса при проектировании СЗИ для гетерогенных информационно-образовательных систем.

Архитектура SIEM-системы защиты информации гетерогенной ИОС

Как уже было отмечено, SIEM-идеология в общем случае обширно охватывает различные аспекты функционирования защищаемой информационно-телекоммуникационной системы и должна быть способна выявлять большое количество разнообразных угроз. Она должна реагировать не только на информационные угрозы, но и на физические, на-

пример, по событиям противопожарной или охранной системы. Однако в случаях проектирования СЗИ для гетерогенных информационно-образовательных систем область охвата событий можно сузить и, как следствие, выделить наиболее существенные задачи, которые должна решать СЗИ на базе SIEM-идеологии:

- выявлять сетевые атаки на ИОС и реагировать на них;
- выявлять попытки несанкционированного доступа к ИОС и реагировать на них;
- выявлять уязвимости в ИСО и реагировать на них;
- выявлять ошибки и сбои в работе ИОС и реагировать на них;
- осуществлять мониторинг работоспособности всех узлов ИОС;
- выявлять некорректное поведение любого из узлов ИОС.

Решение поставленных задач достигается следующим механизмом. СЗИ осуществляет постоянный сбор информации о произошедших событиях от различных источников на всех узлах ИОС, нормализует эту информацию и консолидирует в своей базе данных. Здесь источниками событий могут быть:

- журналы событий (log-файлы) системного и прикладного программного обеспечения (ПО);
- журналы событий брандмауэров на каждом из узлов;
- данные мониторинга аппаратных компонентов узлов ИОС;
- данные мониторинга сетевого трафика;
- журналы аутентификаций на узлах;
- журналы сканеров уязвимостей (например, антивирусного ПО).

После сбора и нормализации событий СЗИ осуществляет их обработку и анализ с целью выявления вектора угрозы. В случаях, если угроза выявлена с высокой долей вероятности, СЗИ должна самостоятельно, с помощью собственной базы знаний, предпринять меры по ее устранению. Если доля вероятности невысока, СЗИ должна оповестить администратора, который будет принимать участие в идентификации угрозы или факта ложного срабатывания с последующей корректировкой базы знаний.

Нами был разработан концепт функциональной модели SIEM-системы защиты информации гетерогенной ИОС, построенной в рамках концепции SIEM-идеологии (рис. 3).

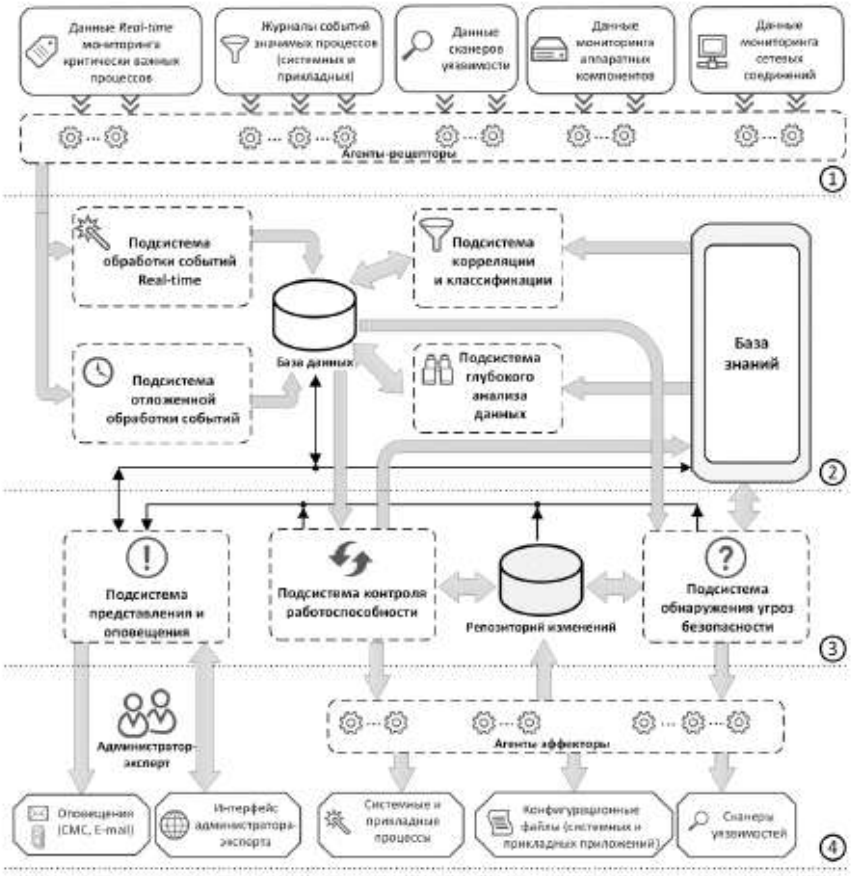

Рис. 3. Концепт функциональной модели SIEM-системы защиты информации гетерогенной ИОС

В данной функциональной модели СЗИ можно выделить четыре укрупненных модуля:

1) модуль сбора событий;

2) модуль обработки и анализа событий;

3) модуль принятия решений и контроля работоспособности;

4) модуль управления информационно-образовательной системой.

Рассмотрим каждый из них более подробно.

Модуль сбора событий является источником исходной (входной) информации о значимых событиях в гетерогенной ИОС. К таким событиям относятся: данные мониторинга критически важных системных и прикладных процессов на всех узлах ИОС (например, показания веб-сервера или СУБД), данные мониторинга аппаратных компонентов узлов (загрузка процессора, объем потребляемой памяти и т. п.), информация о текущем сетевом трафике, записи журналов событий значимых процессов, данные сканеров уязвимостей. Сбор информации происходит с помощью специальных программных агентов-рецепторов, которые работают как службы (daemons) на каждом из узлов ИОС. Все собранные данные передаются на следующий модуль.

Модуль обработки и анализа событий предназначен для фильтрации, нормализации, корреляции, классификации, агрегации в единой базе данных и последующего глубокого анализа данных о событиях. Модуль состоит из нескольких подсистем, каждая из которых реализует часть функционала всего модуля. *Подсистема обработки событий в реальном времени (Real-time)* осуществляет обработку наиболее важной информации, актуальной в текущий момент времени (например, трафик сети или данные мониторинга), и функционирует на каждом из узлов, а *подсистема отложенной обработки событий* осуществляет обработку всех остальных событий на выделенном (одном) узле, но с определенной задержкой.

В этих подсистемах происходит первичная фильтрация, нормализация всех событий и их агрегация в базе данных. *Подсистема корреляции и классификации событий* обеспечивает их первичный анализ и упорядоченную агрегацию в базе данных. *Подсистема глубокого анализа данных* обеспечивает интеллектуальный анализ данных (Data Mining) с целью сокращения объема исходных данных и выявления нетривиальных связей между разнородными событиями в работе ИОС. Эти связи формализуются и также заносятся в базу данных для последующего анализа подсистемой обнаружения угроз.

Модуль принятия решений и контроля работоспособности состоит из несколько подсистем. *Подсистема обнаружения угроз безопасности* на основе уже обработанных и агрегированных данных, а также правил в базе знаний вероятностно выявляет потенциальные угрозы и их векторы (целевые узлы ИОС). Если вероятность идентификации любой из обнаруженных потенциальных угроз превосходит допустимый порог (величина, устанавливаемая экспертом и являющаяся частью правил из базы знаний), то подсистема принимает решение на ее устранение. Решений может быть несколько, и все они носят условно-вероятностный характер. Выбирается то решение, которое имеет наибольшую условную вероятность и не блокировано в базе данных (как неэффективное).

Если таких угроз несколько, то выбирается та, которая имеет наибольшую вероятность. В случаях, когда вероятности обнаруженных угроз ниже допустимого уровня или подсистемой обнаружения не найдено ни одного решения, то возможны следующие действия:

- запуск внешних по отношению к самой СЗИ сканеров уязвимостей с целью уточнения гипотезы о существовании угрозы. После проведения сканирования возможно повышение вероятности угрозы;
- с помощью *подсистемы представления и оповещения* информируется администратор-эксперт СЗИ, который будет сам рассматривать данный инцидент.

Если подсистема обнаружения принимает решение самостоятельно, то перечень необходимых действий для устранения угрозы передается в модуль управления ИОС (который вносит необходимые изменения в работу ИОС) и заносится в специальный *репозиторий изменений* вместе с идентификационными признаками угрозы. Далее на определенный промежуток времени активируется режим карантина. Если в течение данного периода снова обнаруживается та же угроза, то возможны следующие реакции подсистемы обнаружения:

- автоматический выбор другого решения (если оно найдено и удовлетворяет пороговым значениям условной вероятности) и блокирование в базе знаний ранее применяемого;
- оповещение администратора-эксперта СЗИ, который будет принимать решение и в дальнейшем корректировать базу знаний;
- экстренное блокирование работы ИОС в критических случаях с оповещением администратора.

Подсистема контроля работоспособности является своеобразным «надзорным органом» СЗИ и решает следующие задачи:

- контроль работоспособности ИОС, работающей в режиме карантина. В случаях выхода ИОС из работоспособного состояния подсистема осуществляет откат внесенных в работу ИОС изменений (с помощью репозитория), корректировку базы знаний (блокирование соответствующих решений устранения угрозы) и оповещение администратора;
- контроль работоспособности ИОС, работающей в нормальном режиме. В случаях идентификации аномалий в работе происходит оповещение администратора.

Заметим, что под аномалией в работе ИОС здесь подразумеваются события, не связанные с действиями злоумышленников и угрозами информационной безопасности, а имеющие отношение именно к качественным и количественным характеристикам самой ИОС. Так, например, перегрузка узла в результате DDoS-атаки и перегрузка узла в результате значительного, но легитимного роста количества пользователей есть два критериально разных события (т. е. узел просто не справляется с таким увеличением пользователей и, возможно, необходимо внести изменения в архитектуру самой ИОС).

Модуль управления информационно-образовательной системой является инструментом СЗИ, с помощью которого осуществляется исполнение решений подсистемы обнаружения угроз и администратора-эксперта. Как уже было отмечено ранее, под «решением» здесь понимается совокупность действий по устранению угрозы, к которым относятся: изменение конфигурационных файлов системных и прикладных приложений, запуск/остановка/перезапуск системных и прикладных процессов, а также различные команды сканерам уязвимостей. Каждое из действий может быть направлено на конкретный узел или группу узлов ИОС. Мониторинг работы ИОС, управление параметрами работы СЗИ, а также редактирование базы знаний осуществляются через специальный интерфейс администратора-эксперта.

Заключение

Задача обеспечения информационной безопасности гетерогенных информационно-образовательных систем, полноценно использующихся в учебном процессе, является очень важной. Однако задача эта комплексная, в общем случае относящаяся к проблеме обеспечения информационной безопасности распределенных информационных систем, на данный момент не имеющая методов эффективного всеохватывающего решения и требующая новых подходов к проектированию систем защиты информации. Такие СЗИ должны обладать проактивными и интеллектуальными механизмами противодействия возникающим угрозам безопасности.

Одним из подходов к проектированию СЗИ может выступать системообразующая SIEM-идеология, базирующаяся на сборе различных событий (собираемых в процессе работы информационной системы) с последующей их глубокой обработкой с целью выявления угроз безопасности и выработки решений по их устранению. Авторами данной работы был разработан концепт функциональной модели SIEM-системы защиты информации для гетерогенных ИОС, описание которого олицетворяет сценарий ее проектирования. В настоящее время нами, совместно с другими коллегами, ведутся работы по реализации всех подсистем. Так, практически закончена реализация подсистем сбора событий и подсистемы представления и оповещения, базирующихся на свободно распространяемом программном обеспечении с открытым исходным кодом — Zabbix (http://www.zabbix.com). Все остальные подсистемы находятся на стадии исследования и/или разработки.

Разработка систем защиты информации нового поколения, способных к проактивному выявлению потенциальных угроз безопасности и выработке решений по их устранению, является актуальной и очень важной задачей в условиях современного развития гетерогенных информационных систем, сложность архитектуры которых стремительно возрастает, а область применения расширяется.

Литературные и интернет-источники

1. *Бугаев С. Б.* Метод формирования комплекса мер противодействия угрозам информационной безопасности на основе эволюционного подхода // Системы управления и информационные технологии. 2009. № 4 (38).

2. *Ефимов Е. И.* Решатели интеллектуальных задач. М.: Наука, 1982.

3. Информология, информатика и образование: справочное пособие / под общ. ред. В. А. Извозчикова, И. В. Симоновой. СПб.: КАРО, 2004. (Модернизация общего образования.)

4. Искусственные иммунные системы и их применение / под ред. Д. Дасгупты. Пер. с англ. под ред. А. А. Романюхи. М.: ФИЗМАТЛИТ, 2006.

5. *Котенко И. В., Нестерук Ф. Г., Шоров А. В.* Концепция адаптивной защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей // Труды СПИИРАН. 2012. Вып. 4 (23).

6. *Нестерук Ф. Г., Молдовян А. А., Нестерук Г. Ф., Нестерук Л. Г.* Квазилогические нейровечеткие сети для решения задач классификации в системах защиты информации // Вопросы защиты информации. 2007. № 1.

7. Федеральный закон РФ № 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012. http://минобрнауки.рф/документы/2974

8. *Шелестова О.* Что такое SIEM? http://www.securitylab.ru/analytics/430777.php

9. *Шниперов А. Н., Захарьин К. Н.* Вопросы разработки комплексной системы защиты информации для распределенной мультиагентной среды электронного обучения // Информационное противодействие угрозам терроризма. 2012. № 18.

10. *Шниперов А. Н., Захарьин К. Н., Сантьев Е. А.* Вопросы информационной безопасности мультиагентных систем электронного обучения // Материалы Международной научно-технической конференции «Информационные системы и технологии». Красноярск: Изд-во ТТИ Научно-инновационный центр, 2012.

11. *Chen Y., Chen N.* NeuroNet: An Adaptive Infrastructure for Network Security // International Journal of Information, Intelligence and Knowledge. 2009. № 2. Vol. 1.

12. *Miller D. R., Harris Sh., Harper A. A., VanDyke S., Black Ch.* Security Information and Event Management (SIEM) Implementation // McGraw-Hill Companies, 2011.

13. *Negnevitsky M.* Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.