ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ ОБНАРУЖЕНИЯ АТАК НА ОБЪЕКТЫ ИНФОРМАЦИОННОЙ ИНФРУСТРУКТУРЫ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Малюк А.А.[1]

Статья посвящена проблемным вопросам организации и методики анализа, обнаружения и противодействия атакам на объекты информационной инфраструктуры. В первую очередь эти вопросы актуальны для обеспечения безопасности так называемых критических систем, к которым можно отнести государственное и стратегическое управление, энергетику, транспорт, связь, кредитно–финансовую и банковскую сферы. В декабре 2014 года Президентом Российской Федерации утверждена Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Концепция определяет основные принципы создания и функционирования системы, предусматривает формирование нормативно–правового, научно–технического, информационно–аналитического, кадрового и организационно–штатного обеспечения их реализации. Важнейшим элементом этой реализации является решение целого ряда организационно–методических проблем, связанных с исследованием угроз и уязвимостей автоматизированных и информационно–коммуникационных систем критических приложений. В основу анализа, рассматриваемого в статье, положено воздействие атак на технологические циклы управления, приводящее к срыву реализуемых системой задач. Анализ мирового опыта противодействия компьютерным атакам показывает, что последние направлены именно на нарушение технологических циклов управления. В статье предлагается состав основных технологических этапов организации противодействия атакам, суть которых сводится к разработке специальных программных средств, формированию и актуализации баз данных компьютерных атак, формализации возможных сценариев атак, планированию организационно–технических мероприятий и экспериментальной отработке средств анализа и обнаружения атак. Упор делается на создание специальных центров (региональных и отраслевых) анализа и обнаружения компьютерных атак. В заключение приводится перечень первоочередных направлений решения научно–методической проблемы обнаружения атак на объекты кредитно–финансовой сферы.

***Ключевые слова**: компьютерная атака, специальное программно–техническое воздействие, система противодействия атакам, организация противодействия компьютерным атакам, центры анализа и противодействия компьютерным атакам.*

DOI:10.21581/2311-3456-2016-5-8-14

Введение

Как отмечается в Стратегии национальной безопасности, Доктрине информационной безопасности, Военной доктрине Российской Федерации, критические сферы информационной инфраструктуры страны (государственное и стратегическое управление, энергетика, транспорт, связь, кредитно-финансовая и банковская сферы), широко использующие современные информационно-коммуникационные технологии (ИКТ), могут явиться объектами различного рода деструктивных воздействий и террористических посягательств. Так, в Доктрине информационной безопасности Российской Федерации указано, что угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться, в частности, внедренные в аппаратные и программные изделия компоненты, реализующие функции, не предусмотренные документацией на эти изделия; разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем (ИТКС), в том числе и их систем защиты информации.

Вопросам обнаружения и противодействия компьютерным атакам посвящено довольно значительное число исследований, как отечественных, так и зарубежных. Наиболее полный и представительный обзор этих исследований постоянно обновляется фирмой IBM[2]. Однако все исследования, сведения о которых приводятся фирмой IBM, направлены на решение технологических проблем обнаружения атак и реализации тех или иных алгоритмов противодействия им. Аналогичная картина выявляется и при анализе значи-

1 Малюк Анатолий Александрович, к.т.н., профессор, Финансовый университет при Правительстве Российской Федерации, Национальный исследовательский ядерный университет «МИФИ», Москва, AAMalyuk@mephi.ru

2 Исследовательские отчеты фирмы IBM в области обнаружения вторжения: http://www.zurich.ibm/com/.

тельной части опубликованных отечественных работ [1-7]. В то же время чрезвычайно важным является формирование нормативно-правового, организационного и кадрового обеспечения этой деятельности, что подчеркивается утвержденной в 2014 году Президентом Российской Федерации Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[3]. Некоторые подходы к решению этой задачи получили освещение в учебных пособиях [8,9], хотя этого явно недостаточно для реализации упомянутой Концепции.

В связи с этим основное внимание в статье уделяется именно проблеме организационно-методического обеспечения деятельности, направленной на обнаружение компьютерных атак или, другими словами, специальных программно-технических воздействий на объекты информационной инфраструктуры. Такие атаки могут приводить к серьезным нарушениям устойчивости функционирования данных объектов. Если говорить о кредитно-финансовой сфере, являющейся основным предметом статьи, то в нашей памяти еще свежи воспоминания о «черном четверге» 1994 года, когда вскрылись миллиардные мошенничества с бюджетными средствами.

Следует отметить, что по своей сути понятие специальное программно-техническое воздействие является сходным с термином программно-математическое воздействие, введенным Гостехкомиссией России еще в 1997 году при рассмотрении вопросов подключения абонентов государственных органов к сетям общего пользования типа Internet. Учитывая эти соображения, будем определять специальное программно-техническое воздействие (атаку, вторжение) как воздействие на программы и информацию, направленное на нарушение целевых задач автоматизированной системы (АС) и приводящее к несанкционированному изменению технологических циклов управления. Под технологическим же циклом управления будем понимать некоторый набор функций управления, реализуемый конкретной АС или ИТКС.

1. Технологические циклы управления

Основная масса автоматизированных систем, в том числе и в кредитно-финансовой сфере, реализует, в общем, типовой набор функций:

- сбор информации от источников;
- доставка и обмен информацией между абонентами;
- прием и хранение информации у потребителей;
- обработка и визуализация информации;
- выдача информации на исполнительные устройства или органам управления (операторам);
- мониторинг безопасности информации.

Указанные общие функции объединяются в технологические циклы, свойственные только каждой конкретной АС или ИТКС. Анализ отечественных и зарубежных сведений и оценок, упомянутых выше публикаций, имеющейся статистики по компьютерным преступлениям приводит нас к выводу, что именно на нарушение технологических циклов управления и будут направлены атаки, что, как мы уже отмечали, крайне опасно для критически важных объектов. Преднамеренное программно-техническое воздействие на сложную информационную инфраструктуру этих объектов, проведенное как специальная акция с учетом специфики технологических циклов управления, может привести к полной потере управляемости и техногенной или финансовой катастрофе национального масштаба.

Со своей стороны, реализация компьютерных атак предполагает осуществление совокупности организационно-технических мероприятий (планирование, подготовка, маскировка фактов использования комплекса средств программно-технического воздействия). При этом главными объектами атак являются информация, размещенная на носителях или циркулирующая в ИТКС, и программное обеспечение, реализующее обработку данных и функции управления. Таким образом, программное, информационное и техническое обеспечение ИТКС являются непосредственными объектами защиты. Следует иметь в виду, что непосредственными точками осуществления атак служат прежде всего протоколы передачи данных, структуры данных и микропроцессорные устройства.

По своей сути основными формами реализации атак и нарушения порядка функционирования ИТКС могут быть:

- искажение информации;
- введение дезинформации;
- нарушение режимов функционирования;
- блокирование информации;
- разрушение информации;

3 Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утверждена Президентом Российской Федерации 12 декабря 2014 г. № К1274): http://www.scrf.gov/ru/documents/6/131.html.

- перехват информации;
- разглашение информации;
- хищение информации.

Мировой опыт реализации компьютерных атак показывает, что на 80% они совершаются собственными сотрудниками (иногда бывшими) организации или при их непосредственном участии. Именно такие внутренние нарушители информационной безопасности с полномочиями штатного пользователя или администратора системы представляют наибольшую опасность в современной российской действительности.

2. Технологические этапы обнаружения атак

Имея в виду приведенные выше замечания, попробуем сформировать состав основных технологических этапов, реализация которых нацелена на решение проблемы обнаружения атак на системы дистанционного банковского обслуживания (ДБО). Указанный перечень может выглядеть следующим образом:

1. Подготовительный этап: анализ уязвимых мест, оценка сценариев, способов и форм специальных программно-технических воздействий, разработка требований к средствам их обнаружения.
2. Диагностика и экспертиза критически важных объектов системы ДБО.
3. Выбор (разработка) средств обнаружения воздействий.
4. Встраивание в АС ДБО и настройка датчиков воздействий.
5. Актуализация базы данных компьютерных атак на системы банковского обслуживания.
6. Сбор информации от датчиков.
7. Анализ результатов мониторинга системы ДБО.
8. Обнаружение воздействий.
9. Противодействие специальным программно-техническим воздействиям.
10. Технико-экономическая оценка эффективности применения средств обнаружения воздействий.

Организационно анализ и обнаружение атак на систему ДБО можно осуществить путем формирования технологического шаблона диагностики объектов и проведения на его основе экспертизы информационной безопасности. Технологический шаблон должен позволить в общем случае декомпозировать защищаемую систему на ряд основных объектов, среди которых можно выделить:

- средства удаленного доступа и фильтрации сетевого трафика на основе межсетевых экранов и виртуальных частных сетей;
- автоматизированные рабочие места (АРМ) приложений;
- сервер и клиенты электронной почты;
- коммуникационное оборудование локальной вычислительной сети (ЛВС);
- сервер баз данных;
- программно-технические средства защиты информации от несанкционированного доступа и компьютерных вирусов.

Суть предлагаемого решения рассматриваемой проблемы заключается в том, что в состав ИТКС системы ДБО включаются специально разработанные программные средства анализа и обнаружения атак с учетом специфики технологических циклов управления системы как дополнение к межсетевым экранам, виртуальным частным сетям и другим сертифицированным средствам сетевой защиты.

Необходимость разработки специализированных средств анализа и обнаружения атак обусловлена тем, что, как свидетельствует статистика, известные коммерческие средства такие, как I*SS, NetRanger, CyberCop, Omni Guard/ITA,* загружают от 20 до 50% сетевого трафика. При этом они фактически не учитывают особенности технологических циклов сбора, обмена и доставки информации в конкретных ИТКС (в нашем случае в системе ДБО). Например, в ISS включены около 700 сценариев атак. Хотя в реальной ИТКС системы ДБО максимально возможных сценариев нарушения процессов управления порядка 20-30. Такое заключение можно сделать на основе анализа имеющейся открытой информации по атакам на банковские системы. В связи с этим весьма актуальна разработка программных средств анализа и обнаружения атак, которые могут быть интегрированы с системой ДБО. Они должны быть компактны по своим функциям и надежно осуществлять контроль технологических циклов управления системой и регламентов обработки информации.

Если говорить в целом о создании методов и технологии обнаружения атак, то необходимо еще выделить требующие своего решения следующие проблемные вопросы:

- разработка унифицированных средств анализа и обнаружения атак;
- формирование и актуализация базы данных компьютерных атак;
- формализация возможных сценариев атак;
- планирование организационно-технических мероприятий по способам, формам, методам и средствам противодействия атакам;
- экспериментальная отработка средств ана-

лиза и обнаружения атак.

3. Методическое обеспечение и организационные мероприятия

Методическое обеспечение и организационные мероприятия по обнаружению атак в соответствии с Концепцией государственной системы [9] должны разрабатываться в рамках решения всего комплекса задач обеспечения безопасности информации ИТКС. Отсюда следует, что в их состав необходимо включить три группы методик и мероприятий:

Первая группа:

- методика обнаружения атак на основе комбинированного метода обнаружения технологических циклов управления в конкретной ИТКС (в нашем случае – это система ДБО);
- модель угроз ИТКС (уточненные перечни угроз, уязвимых мест, сценарии и характеристики средств программно-технического воздействия, модель нарушителя).

Вторая группа:

- план организационных мероприятий по обнаружению атак;
- комплексная технология обнаружения и анализа вторжений в ИТКС;
- методы выявления программно-технических воздействий в протоколах обмена и специализированных базах и хранилищах данных;
- инфологическая модель баз данных компьютерных атак.

Третья группа:

- проект технического задания на разработку средств обнаружения атак;
- проведение экспериментальной отработки средств обнаружения с использованием соответствующей имитационной модели;
- внедрение средств обнаружения вторжений в ИТКС;
- метод оценки эффективности обнаружения атак.

Последнюю из приведенных нами проблему, а именно проблему разработки метода оценки эффективности обнаружения вторжений, можно решить с помощью подхода, основанного на вероятностной экспертно-математической оценке событий обнаружения нарушений на рубежах защиты. Возможными показателями оценки такой эффективности могут служить:

- коэффициенты эффективности обнаружения воздействий на данном рубеже защиты установленными средствами анализа и обнаружения атак;
- вероятности преодоления / непреодоления средствами воздействия рубежей защиты (определяемые с учетом принятых параметров средств обнаружения, угроз безопасности информации, уязвимых мест, характеристик потенциального нарушителя, возможных методов и средств реализации угроз);
- шкала коэффициентов оценки ущерба от реализации атак.

Ключевой организационной и научно-методической проблемой реализации процессов отработки совокупности организационно-технических мероприятий и средств анализа и обнаружения воздействий на реальных объектах ИТКС является экспериментальная отработка средств обнаружения вторжений. Существо данной проблемы заключается в том, что для проверки выполнения требований к средствам обнаружения и противодействия вторжениям и доведения этих средств до реальных образцов необходимо воспроизвести информационную среду функционирования ИТКС как объекта защиты, произвести имитацию средств и сценариев поведения нарушителя, а также действий лиц, принимающих решения по обеспечению устойчивости функционирования ИТКС и нейтрализации (противодействию) компьютерным атакам. Особую методическую и техническую сложность представляет моделирование ситуации, когда при осуществлении атаки используются программно-технические закладки и недекларированные возможности на основе внедрения программно-технических средств, замаскированных под штатные.

В отсутствие полной и достоверной базы данных по реальным, имевшим место вторжениям, решающую роль играют неформальные методы на основе осуществления массовой экспертизы. Для ее осуществления, очевидно, потребуется создание специальных экспериментальных центров анализа и обнаружения компьютерных атак. Целью создания таких центров является обеспечение практической направленности работ по созданию образцов средств анализа и обнаружения вторжений, отработке организационно-технических мероприятий и проверке средств анализа, обнаружения и противодействия компьютерным атакам, а также испытаний перспективных ИТКС в защищенном исполнении.

Центры должны обеспечивать отработку планов организационно-технических мероприятий, проведение научно-технического обоснования, разработку технических требований, структуры, принципов построения и функционирования средств анализа, обнаружения и предупреждения компьютерных атак, проведение испытаний защи-

щенных технологий на основе математического, имитационного и натурного моделирования.

Следует отметить, что попытка создания подобных центров была предпринята в России еще в 1997 году на основе реализации программы развития исследований по проблемам обеспечения информационной безопасности в системе высшей школы [10]. Аналогичные решения пытаются проводить и США, реализуя программу защиты своей критически важной информационной инфраструктуры (компьютерных сетей и систем связи) от компьютерных атак, отрабатывая в рамках этой программы методы и средства информационного противодействия потенциальным угрозам. Работы по созданию системы раннего предупреждения об информационном нападении на национальную информационную инфраструктуру страны начались в США в 1998 году в соответствии с директивой президента США.

Представляется, что накопленный в высшей школе России опыт и действующие на сегодня центры информационной безопасности (всего 29 центров, охватывающих все Федеральные округа) вполне могут явиться организационной основой региональной системы анализа атак на объекты кредитно-финансовой сфера, тем более, что многие из этих центров имеют тесные связи с соответствующими территориальными подразделениями Банка России.

4. Программно-техническое обеспечение

Решение проблемы обнаружения атак должно опираться на соответствующее обеспечение, в общем случае включающее три ключевых элемента:

- программно-аппаратные средства для реализации информационно-моделирующей базы и экспериментальных участков ИТКС;
- специализированные серверы сбора данных о компьютерных атаках;
- средства обнаружения воздействий, администрирования безопасности ИТКС и визуализации информации.

Сценарий отработки организационно-технических мероприятий по обнаружению атак может быть представлен следующей последовательностью действий:

1. Аналитическое обоснование средств обнаружения атак.
2. Разработка требований к составу и функциям средств обнаружения атак.
3. Разработка средств анализа и обнаружения атак.

Проведение экспериментов по отработке сценариев анализа и обнаружения атак (имитация воздействий, обнаружение атак, визуализация, противодействие компьютерным атакам и технико-экономическая оценка).

Базовая структура разрабатываемых программно-технических средств обнаружения атак должна включать в свой состав следующие средства:

- комплекс средств реализации атак;
- программы датчиков общего и специального программного и технического обеспечения;
- программы серверов и абонентов сбора данных;
- сервер баз данных компьютерных атак;
- программы обнаружения атак;
- программы визуализации;
- программы администрирования и управления датчиками.

В настоящее время практическое применение находят два способа обнаружения атак – выявление аномального поведения и выделение фактов нарушений на основе сигнатурного анализа. Представляется целесообразным при разработке ИТКС в защищенном исполнении использовать комбинированный метод выявления вторжений, который состоит во взаимосвязанном применении анализа сигнатур, анализа скриптов (функций), анализа технологических циклов управления в ИТКС и организационно-технического контроля. При этом организационно-технический контроль позволяет производить проверку различных источников информации о событиях в ИТКС и выявлять подозрительную активность абонентов и нарушения в системе по совокупности косвенных признаков.

В рамках создания ИТКС в защищенном исполнении для сферы ДБО должны быть также предусмотрены работы по визуализации результатов обнаружения атак на объекты ИТКС на основе комплексного использования современных технологий и, возможно, данных геоинформационных систем.

5. Гипотетический пример

В заключение в качестве примера рассмотрим, как могут выглядеть методика и состав средств обнаружения атак на ИТКС для случаев: «воздействие на соединение абонентов» и «отказ в обслуживании». Выявление вторжений осуществляем на основе контроля технологических циклов управления ИТКС: обмена информацией, доставки информации, сбора информации и предоставле-

ния потребителям с отображением результатов в виде 3D-объектов в vrml-формате. Фиксирование факта нарушения безопасности осуществляем по критическому порогу событий безопасности и выявлению моментов времени, когда информация по плану не могла поступать или превышению граничного значения принятого объема данных, а также ложным адресам абонентов сети и неверной сенсорной информации. Для визуализации трехмерной информации об ИТКС нам потребуются априорная разработка их графических образов и размещение в базе данных, создание специализированных интерфейсов с геоинформационными системами и средствами компьютерной графики.

Выводы

Таким образом, проведенный нами анализ подходов к решению организационных и методических проблем обнаружения атак на объекты информационной инфраструктуры системы ДБО показывает, что в целом формирование информационно-моделирующей базы обнаружения вторжений и создание средств обнаружения находится на уровне формирования соответствующих структур и начальной методической проработки проблемных вопросов. Поэтому в качестве первоочередных направлений решения научно-методической проблемы обнаружения атак на объекты информационной инфраструктуры можно предложить следующее:

• создание ведомственного и региональных центров анализа и обнаружения компьютерных атак с учетом специфики кредитно-финансовой сферы и деятельности федеральных и региональных структур, разработка положения по их взаимодействию (как отмечалось, здесь вполне может быть использован опыт создания региональных центров информационной безопасности в системе высшей школы);

• формирование программы создания отечественных средств обнаружения вторжений и мониторинга ИТКС (это мероприятие имеет первостепенное значение в плане реализации стратегии импортозамещения и конечно же относится не только к кредитно-финансовой, но и к другим сферам критических приложений);

• организация работ по импортозамещению на основе использования коммуникационного и компьютерного оборудования отечественного производства, защищенных ИТКС со встроенными средствами обеспечения устойчивости функционирования в условиях воздействия преднамеренных и непреднамеренных угроз информационной безопасности;

• подготовка нормативно-технических документов, определяющих типовые требования к разработке и применению отечественных средств анализа, обнаружения и противодействия компьютерным атакам;

• организация постоянно действующего научно-практического семинара по отечественным средствам анализа и обнаружения вторжений (возможно на базе одного из существующих центров информационной безопасности ведущих вузов, например, МГТУ им. Н.Э.Баумана).

***Рецензент**: Дворянкин Сергей Владимирович, доктор технических наук., профессор, заместитель заведующего кафедрой «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, SVDvoryankin@fa.ru*

Литература

1. Камие В.А., Натров В.В. Методология обнаружения вторжений // Известия Волгоградского государственного технического университета. 2006. № 4. С. 148-153.
2. Поздняков С.А. Использование схемы совпадений в системах обнаружения вторжений на основе нейронных сетей // Вестник Омского университета. 2012. № 2 (64). С. 189-190.
3. Тишина Н.А., Дворовой И.Г., Соловьев Н.А. Обнаружение вторжений на основе вейвлет-анализа сетевого трафика // Вестник Уфимского государственного авиационного технического университета. 2010. Т. 14. № 5 (40). С. 188-194.
4. Бурлаков М.Е. Модель многослойной универсальной системы обнаружения вторжений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 214-218.
5. Половко И.Ю., Пескова О.Ю. Анализ функциональных требований к системам обнаружения вторжений // Известия ЮФУ. Технические науки. 2014. № 2 (151). С. 86-92.
6. Котов В.Д., Васильев В.И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник Уфимского государственного авиационного технического университета. 2012. Т. 16. № 3 (48). С. 198-204.
7. Мазиков К.И. Анализ современных сертифицированных средств обнаружения вторжений в информационных сетях // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2014. Т. 19. № 2. С. 661-662.
8. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. М.: ЮНИТИ-ДАНА, 2001. 587 с.
9. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). М.: Горячая линия–Телеком, 2013, 220 с.
10. Малюк А.А., Герасименко В.А., Милославская Н.Г. и др. Проблемы создания и организации работы центров защиты информации // Безопасность информационных технологий. 1997. № 4. С. 5-61.

 УДК 004.732.056 (075.8)

ORGANIZATIONAL AND METHODOLOGICAL PROBLEM OF DETECTING ATTACKS ON OBJECTS OF INFORMATION INFRASTRUCTURE OF CREDIT AND FINANCIAL SPHERE

Anatoly Malyuk[4]

The article is devoted to the topical issues of organization and methods of analysis, detection and counteraction to attacks on the objects of information infrastructure. First of all these issues are relevant to ensure the security of so-called critical systems, which include the public and strategic management, energy, transport, communications, credit and financial and banking spheres. In December 2014, President of the Russian Federation approved the Concept of the state system of detection, prevention and elimination of consequences of cyber attacks on information resources of the Russian Federation. The Concept defines the basic principles of establishment and functioning of the system, and provides the formation of legal, scientific, technical, information-analytical, organizational and staffing maintenance to ensure their implementation. The most important implementation element is to solve a number of organizational and methodological problems related to the investigation of the threats and vulnerabilities of automated and information and communications systems of critical applications. As the basis of analysis, considered in the article, the impact of attacks on the technological cycles of control, leading to the disruption of tasks solved by the system, is taken. Analysis of the world experience of countering computer attacks shows that they are directed to the violation of technological control loops. The article proposes the structure of the basic technological stages of organization to counter attacks, which essentially means the development of special software, creation and updating of the database of computer attacks, formalization of possible attack scenarios, planning of organizational and technical measures and experimental development of analysis and intrusion detection tools. The emphasis is made on the creation of special centers (regional and sectoral) for analysis and detection of computer attacks. Finally, a list of priority directions of scientific and methodological problems› decision for detecting attacks on the objects of credit and financial sphere is given.

Keywords*: computer attack, special software and technical effects, intrusion detection, attacks› countering system, organization of countering computer attacks, centers for analysis and detection of computer attacks.*

References

1. Kamie V.A., Natrov V.V. Metodologiya obnaruzheniya vtorzheniy, Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. 2006. No 4, pp. 148-153.
2. Pozdnyakov S.A. Ispol'zovanie skhemy sovpadeniy v sistemakh obnaruzheniya vtorzheniy na osnove neyronnykh setey, Vestnik Omskogo universiteta. 2012. No 2 (64), pp. 189-190.
3. Tishina N.A., Dvorovoy I.G., Solov'yev N.A. Obnaruzhenie vtorzheniy na osnove veyvlet-analiza setevogo trafika, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2010. T. 14. No 5 (40), pp. 188-194.
4. Burlakov M.E. Model' mnogosloynoy universal'noy sistemy obnaruzheniya vtorzheniy, Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2014. No 2 (32), pp. 214-218.
5. Polovko I.Yu., Peskova O.Yu. Analiz funktsional'nykh trebovaniy k sistemam obnaruzheniya vtorzheniy, Izvestiya YuFU. Tekhnicheskie nauki. 2014. No 2 (151), pp. 86-92.
6. Kotov V.D., Vasil'yev V.I. Sovremennoe sostoyanie problemy obnaruzheniya setevykh vtorzheniy, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2012. T. 16. No 3 (48), pp. 198-204.
7. Mazikov K.I. Analiz sovremennykh sertifitsirovannykh sredstv obnaruzheniya vtorzheniy v informatsionnykh setyakh, Vestnik Tambovskogo universiteta. Seriya: Estestvennye i tekhnicheskie nauki. 2014. T. 19. No 2, pp. 661-662.
8. Miloslavskaya N.G., Tolstoy A.I. Intraseti: obnaruzhenie vtorzheniy. M.: YuNITI-DANA, 2001. 587 P.
9. Shelukhin O.I., Sakalema D.Zh., Filinova A.S. Obnaruzhenie vtorzheniy v komp'yuternye seti (setevye anomalii). M.: Goryachaya liniya–Telekom, 2013, 220 P.
10. Malyuk A.A., Gerasimenko V.A., Miloslavskaya N.G. i dr. Problemy sozdaniya i organizatsii raboty tsentrov zashchity informatsii, Bezopasnost' informatsionnykh tekhnologiy. 1997. No 4, pp. 5-61.

4 Anatoly Malyuk, Ph.D., Professor, Financial University under the Government of the Russian Federation, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, AAMalyuk@mephi.ru