УДК 004.056.53:004.492.3 (045)

ПАРАМЕТРЫ ПРОГНОЗИРОВАНИЯ И ИДЕНТИФИКАЦИИ АТАК В ИНФОРМАЦИОННО-КОМУНИКАЦИОННЫХ СИСТЕМАХ

Валерий Азарсков, Андрей Гизун, Андрей Грехов, Сергей Скворцов

Вопросы, связанные с прогнозированием, мониторингом и выявлением кризисных ситуаций в информационно-коммуникационных системах, имеют большое научное и практическое значение. В концепции управления беспрерывностью бизнеса эти процессы занимают центральные позиции, определяя возможности всех используемых механизмов в сфере возобновления бизнес-процессов и защиты информационных ресурсов в условиях влияния кризисных ситуаций. Любая кризисная ситуация является последствием совокупности инцидентов или атак. Исходя из этого определения и формализации основных параметров, которые могут быть использованы для выявления и идентификации компьютерных атак, безусловно, являются актуальной задачей. Именно этим вопросам посвящено это исследование. Так, четкое определение множества параметров, снимаемых как на сетевом, так и локальном уровне, позволит учитывать особенности каждой кризисной ситуации, атаки или инцидента информационной безопасности и, как следствие, повысить эффективность систем защиты и превентивных средств. Основные результаты работы могут быть использованы для построения системы прогнозирования, выявления и идентификации компьютерных атак в информационно-коммуникационных системах на базе методов нечеткой логики.

Ключевые слова: *кризисная ситуация, идентификация кризисных ситуаций, информационно-коммуникационная система, нечеткая логика, кортеж, параметр, управление беспрерывностью бизнеса, информационные ресурсы, компьютерные атаки.*

Вступление. В настоящее время управление непрерывностью бизнеса (УНБ) представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента современного предприятия. Актуальность этого направления для каждой компании объясняется необходимостью обеспечить выживание и сохранение своего бизнеса в кризисных ситуациях (КС). Под термином управление непрерывностью бизнеса обычно понимается системный процесс оценки последствий возникших КС и принятия надлежащих решений по сохранению бизнеса компании. В этой ситуации вопросы обеспечения непрерывности бизнеса были восприняты международными и национальными компаниями с большой готовностью. При этом большинство именно небольших и средних предприятий находятся в серьезной зависимости от различных угроз, которые могут прервать их бизнес-процессы и особенно движение денежных средств.

Концепция УНБ предусматривает ряд этапов, наиболее важными среди которых есть анализ влияния на бизнес, прогнозирование и идентификация КС, реагирование на КС, устранение их последствий и восстановление бизнес-процессов, прерванных КС, а также документальное обеспечение систем УНБ. Анализ работ [1-3] и стандартов УНБ [4-7] показал достаточное развитие на сегодняшний день систем восстановления бизнес-процессов и систем документирования планирования УНБ. Но, в тоже время, системы прогнозирования и идентификации КС находятся на начальной стадии развития, и их эффективность является сомнительной с точки зрения практического применения. Для развития этого направления, прежде всего, нужно привести дефиницию понятия КС, выделить наиболее актуальные виды атак в информационно-коммуникационных системах (ИКС), потенциально приводящие к возникновению КС и формализировать параметры, которые могут быть использованы для прогнозирования и идентификации атак.

Статистические данные подтверждают актуальность борьбы с КС и атаками на ИКС, порождающими их, особенно связанных со средой Интернет. Так Украина попала в группу стран повышенного риска по возможности заражения при серфинге в Интернете. В эту группу с результатом 41-60% вошли первые 15 стран из TOP 20. Это Россия, Австрия, Германия, большинство стран постсоветского пространства и страны Азии. Эта группа уменьшилась более чем вдвое: по итогам 2012 года в нее входила 31 страна (Украина находится на 9 месте с 45,66% уникальных пользователей, которые подвергались веб-атакам) [8, 9].

Анализ существующих публикаций. Общие принципы и понятия УНБ описаны в международных и национальных стандартах, а также в работах, названых выше. В работе [10] приведено определение понятия КС, которое мы будем использовать в нашем исследовании: кризисная ситуация в аспекте непрерывности бизнеса – это

определенная ситуация или событие, имеющее место на некоторой территории (организации, предприятии), потенциально способна нанести серьезный ущерб организации, привести к нарушению деятельности организации, потери услуг или функций предприятия в достаточном объеме чтобы угрожать жизнеспособности организации. Вопросы классификации КС проработаны в работе [11], где выделены наиболее важные характеристики для их классификации. Наибольший интерес для нас представляет классификация КС относительно причин их происхождения (источника), где выделены такие типы как КС природного, техногенного, социального, экономического и экологического характера, которые, в свою очередь, делятся на подтипы. Далее в исследовании будем работать с КС техногенного характера в системах связи и телекоммуникаций, то есть в информационно-коммуникационных системах. Кроме того в практике УНБ ЕМС, рассмотренной в [1], выделена отдельная категория ИБ-инцидентов, куда включены киберпреступность, компьютерные вирусы и несостоятельность ИКС. Также следует выделить работу [12], где произведена, по аналогичному принципу, формализация параметров, необходимых для идентификации нарушителя информационной безопасности и их категоризации на определенные типы, а также [13], где рассмотрены параметры для систем выявления атак в ИКС. Описанные в этих работах параметры предназначены для других целей, по сравнению с нашей работой, поэтому целесообразно некоторые из них пересмотреть и пополнить новыми выделенными параметрами.

Основная цель исследования. Для эффективного предупреждения КС в сфере ИБ необходимо разработать набор ключевых параметров для прогнозирования и идентификации атак на ИКС, которые при определенных условиях могут быть причинами возникновения кризиса. Таким образом, целью данной работы есть определение (формализация) основных параметров, значение и характер изменения которых могут определить возможность реализации той или иной атаки.

Основная часть. Определение конкретной КС и их характеристик в большей мере является субъективным. Среди основных причин возникновения КС центральное место занимают инциденты ИБ и атаки на ИКС. В общем, в контексте этой работы, основываясь на предложенной классификации [11], практике УНБ ЕМС, статистике КС и инцидентов информационной безопасности [8, 9, 14, 15], целесообразно выделить такие виды атак в ИКС: DDos-атака, спам, сканирование портов, компьютерный вирус (среди которых можно выделить такие подвиды как сетевой червь и троянская программа) программы–блокировщики (баннеры), тесно связанные с понятием фишинга. Каждому из этих видов атак свойственны определенные параметры (характеристики), контролируя которые, можно их предсказать и идентифицировать.

Рассмотрим более детально особенности выделенных атак в ИКС, описанные в табл. 1.

Чтобы спрогнозировать возможность реализации атаки или выявить ее и идентифицировать необходимо разработать систему, которая будет производить мониторинг сетевых характеристик (параметров трафика) и локальных характеристик (параметров компьютерной системы или хоста), приведенные в табл. 2. Учитывая то, что реализация КС может иметь как предопределенный так и случайный характер, а ИКС есть по своей сути слабоформализованной средой, то система должна быть основана на специальных методах теории нечетких множеств [16], а следовательно некоторые из используемых параметров могут быть нечеткими по своей природе. Рассмотрим и проанализируем параметры, контролируемые системой для прогнозирования, выявления и идентификации атак в ИКС:

1) Загрузка ЦП, CPU – процентный показатель процессорного времени, выделенного на выполнение задач. Основные причины загрузки процессора - программные. Это либо большое количество запущенных одновременно программ, либо вирус. Также загруженность процессора может быть не программная, а аппаратная. Большая загрузка процессора указывает на то, что в компьютере выполняется какое-либо действие, а по уровню загруженности можно определить, насколько сильно компьютер подвержен вредоносным воздействиям. Параметр является нечетким, так как загрузка центрального процессора изменяется каждую секунду, ее оптимальное (нормальное) значение различно для разных систем и, к тому же, не дает четкого ответа о наличии факта атаки.

2) Загруженность сетевого канала, CNCh. Параметр связан с понятием трафика – это объем информации, который проходит через сервер за определенный период времени. Трафик бывает входящим – данные, получаемые компьютером; исходящим – данные, отправляемые компьютером; внутренний – в пределах определенной сети, чаще всего локальной), внешний – за преде-

лами определенной сети, чаще всего Интернет-трафик. Мониторинг трафика позволяет фиксировать данные, которые передаются по интернет-каналу. Значительное возрастание трафика свидетельствует о возможной DDos-атаке или другой атаки. А поскольку величину нормальной загруженности сетевого канала определить практически невозможно, то параметр есть нечетким.

Таблица 1

Описание атак на ИКС

Атака	Возможный ущерб	Сложность в реализации	Скорость реализации	Особенности реализация кризисной ситуации
DDos атака	Максимальный	Очень сложно	Достаточно долго	Воздействует на конкретную цель (сервер, хост ИКС)
Спам	Минимальный / средний	Просто	Быстро	Воздействует на множество целей (рабочих станций ИКС)
Сканирование портов	Средний	Просто	Средне, в зависимости от параметров сканирования	Воздействует на множество портов локального хоста или сети
Вирус	Разной степени, в зависимости от типа	Разной степени, в зависимости от типа	Разной степени, в зависимости от типа	Воздействует как на отдельный хост, так и на все хосты сети
Сетевой Червь	Минимальный	Просто \ Средне	Быстро	Воздействует как на отдельный хост так и на все хосты сети
Троянский конь	Очень высокий	Сложно	Средне	Воздействует как на отдельный хост так и на все хосты сети
Программы – блокировщики (баннеры)	Средний	Выше среднего	Быстро	Воздействует на конкретный хост ИКС

3) Несвойственные процессы, UPr. Используемые процессы на хосте ИКС являют собой совокупность системных и пользовательских выполняющихся программ, имеющих полный набор регистров, которые находятся в процессоре и занимающих внешние ресурсы, такие как дисковое пространство, устройство ввода вывода, канал передачи информации и другие. Наблюдая за количеством процессов, можно определить какой процесс есть новым, и может быть вредоносным. Параметр является точным, так как количество процессов ограничено, в начале работы система мониторинга делает так называемый снимок системы и новые процессы всегда можно просмотреть и перечислить.

4) Размер временных файлов, STF. Это величина, демонстрирующая, сколько места временный файл занимает на диске. Временный файл – файл, создаваемый определённой программой или операционной системой для сохранения промежуточных результатов в процессе функционирования или передачи данных в другую программу. Обычно такие файлы удаляются автоматически создавшим их процессом. Здесь может храниться копия вируса, либо резервное тело вируса для автоматического запуска. Параметр является нечетким из-за того что слишком много разных временных файлов создаётся и удаляется во время работы компьютера и размер их при нормальном функционировании может быть различным.

Таблица 2

Параметры для выявления и идентификации атак

Параметр	DDos-атака	Спам	Сканирование портов	Компьютерные вирусы		Баннер	Нечеткость
				Сетевой червь (Вирус)	Троянский конь		
CPU	В	С	С	ВС	ВС	С	+
CNCh	ОВ	В	В	С/ВС	ВС	С/ВС	+
UPr	О	О	О	П	П	П	-
STF	С	С	С	В	ВС	С	+
OUP	П	П	О	П	П	О	-
MU	В	В/С	С/Н	В	В/С	С/Н	+
NEr	ВС	ВС	С	ВС	ВС	ВС	+
ChSSF	О	О	О	П	П/О	П	-
NCC	В	С/ВС	С/ВС	С	С	С	+
DbR	Н	С	Н	С	С	С	+

ОВ – очень высокая; В – высокая; ВС – выше среднего; С – средняя; Н – низкая; О – отсутствует; П – присутствует.

5) Открытие неиспользуемых портов, OUP. Порт – это параметр протоколов TCP и UDP. Может быть открытым либо закрытым. Закрытыми называются те порты, с которыми не удается создать соединение. Следовательно, открытым портом называют порты, с которыми возможно установить соединение. Через открытый порт злоумышленник может подключится к удаленному ПК, либо же загрузить или скачать файлы без ведома пользователя. Параметр является четким, так как существует ограниченное количество портов, которые используются операционной системой, выделенных и зарегистрированных IANA (Internet Assigned Numbers Authority). Так вначале работы системы мониторинга делается снимок системы (открытые порты), а появление в процессе работы новых открытых портов может служить сигналом о атаке на ИКС.

6) Загруженность оперативной памяти, MU – это показатель количества занятых структурных единиц оперативной памяти. В оперативной памяти информация хранится временно и при отключении питания удаляется. В ней хранится информация следующего рода: системная информация, необходимая для работы операционной системы; информация от устройств, подключённых к компьютеру и их драйвера; антивирусы, вирусы, резидентные программы; программы и файлы, которые в данный момент открыты и находятся в обработке. Параметр является нечетким, так как загруженность оперативной памяти изменяется каждую секунду, ее оптимальное (нормальное) значение различно для разных систем и к тому же не дает четкого ответа о наличии атак в ИКС.

7) Количество сбоев и ошибок, NEr. Ошибка в ИКС – это ненормальная ситуация, которая может привести к снижению или потере способности функционального узла к выполнению предопределенной функции, то есть к отказу. Этот параметр относится к нечетким, так как ошибки очень часто являются элементом нормальной работы системы в ИКС из-за технических характеристик аппаратного и программного обеспечения. В эту группу входит широкий спектр событий от ошибок при авторизации к сбоям при выполнении определенных процессов или файлов. При атаке в ИКС, независимо от ее вида, частота появления неисправностей будет несколько выше. Так большая интенсивность возникновения ошибок и сбоев свидетельствует с некоторой вероятностью о возможности реализации атак.

8) Изменений структуры и размера файлов, ChSSF. Этот параметр наиболее важен для идентификации компьютерных вирусов, так как те очень часто изменяют структуру файла, вписывая свое тело в начало, конец или середину файла, и структуру файловой системы. Так, существует классификация, по которой выделяют: 1) файловые вирусы, которые располагаются в файлах различных форматов (COM, EXE, SYS, DOC и др.) и, как правило, инициализируются первыми при их обработке, 2) загрузочные вирусы, располагающиеся в Boot-секторах дисков или в секторе винчестера с системным загрузчиком и активизирующиеся при начальной загрузке ОС и 3) файлово-загрузочные вирусы, являющиеся сочетанием двух предыдущих групп и инфицирующие как файлы, так и указанные выше сектора, а алгоритм их работы значительно усложняется с учетом бинарного действия. Этот параметр есть четким при условии, что процессы работы легальных пользователей постоянно контролируются и регламентированы правилами политики безопасности в ИКС.

9) Количество одновременных подключений, NCC. Как показывает практика для эффективного проведения DDoS необходимо привлечение большого количества источников, участвующих в нападении на жертву. Следовательно, параметр **NCC** при увеличении количества подключений к серверу может использоваться в качестве одного из признаков начала атаки. Максимальное число подключений, которое может поддерживать сервер, зависит от его аппаратных и программных возможностей и характеризуется параметром maxNCC, значение которого будет отличаться для разных серверов [13]. Параметр является нечетким, так как при небольших значениях характерен и для состояния нормального функционирования и точное значение, которое может свидетельствовать об атаке, определить практически невозможно.

10) Задержка между запросами от одного источника, DbR. Параметр характеризует время между последовательными запросами от одного подключенного к серверу клиента. На некоторых серверах, для предотвращения атак, этот параметр устанавливается вручную (например, 1 запрос за 1 секунду от пользователя). Уменьшение задержки между запросами может свидетельствовать о начале DDoS-атаки, целью которой является отправка как можно большего количества запросов, которые выведут сервер из работоспособного состояния. Значение параметра опреде-

ляется величиной maxDbR, которая зависит от программного обеспечения и назначения сервера [13]. Этот параметр также есть нечетким.

Рассмотренные в работе параметры создают по аналогии с [12, 17] кортеж выявления и идентификации атак:

DIA = <CPU, CNCh, UPr, STF, OUP, MU, NEr, ChSSF, NCC, DbR>.

Значение элементов этого кортежа дают возможность выявить атаку в ИКС и идентифицировать ее относительно выделенных видов: DDos-атака, спам, сканирование портов, сетевой червь (вирус), троянская программа, программы–блокировщики (баннеры).

Выводы. Таким образом, в этом исследовании определено значение параметров кортежа выявления и идентификации атак DIA, которые должны контролироваться системой для прогнозирования атак на ИКС, их фиксации и реагирования на них. Формализация этих параметров разрешает учитывать особенности атак в ИКС и увеличить эффективность превентивных средств и систем защиты информационных ресурсов. Это также может быть использовано для выявления КС на раннем этапе их развития. В следующих работах предложенные параметры и их кортеж будут использованы как базис для построения эффективной системы прогнозирования и идентификации атак и КС. Также отметим, что количество выявляемых атак в ИКС и перечень параметров могут быть изменены при реализации системы в зависимости от требований к ее функциональности.

ЛИТЕРАТУРА

[1]. Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляев. – М.: ДМК Пресс, Компания АйТи, 2011. – 400 с.

[2]. Van Bon Jan. ИТ СЕРВИС–МЕНЕДЖМЕНТ. Вводный курс на основе ITIL / Jan Van Bon. – Van Haren Publishing, по заказу ITSMF Netherlands, 2003. – 72 с.

[3]. Harris S. CISSP Certification All-in-One Exam Guide. – 5th edition. – Mc Graw-Hill Osborne Media, 2010. – 1216 p.

[4]. Business continuity management. Code of practice: BS25999-1:2006 – BSI British Standards, 2006 – 28 p.

[5]. Business continuity management. Specification: BS25999-2:2007 – BSI British Standards, 2007. – 38 p.

[6]. Singapore Standard for Business Continuity Management: SS540:2008 – SPRING Singapore, 2008. – 54 p.

[7]. Business continuity – Managinig disruption-related risk: AS/NZS 5050 – Standards Australia, 2010. – 53 p.

[8]. Гудкова Д. Kaspersky Security Bulletin. Спам в 2013 году [Електронний ресурс]: стаття / Д. Гудкова. – Режим доступу: http://www.securelist.com/ru/analysis/208050828/Kaspersky_Security_Bulletin_Spam_v_2013_godu

[9]. Гарнаева М., Kaspersky Security Bulletin 2013. Основная статистика за 2013 год [Електронний ресурс]: стаття / Мария Гарнаева, Кристиан Функ – Режим доступу: https://www.securelist.com/ru/analysis/208050822/Kaspersky_Security_Bulletin_2013_Osnovnaya_statistika_za_2013_god

[10]. Гізун А.І. Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної науково-технічної конференції «АВІА-2011». – К.: НАУ, 2011. – Т1 – с. 2.5-2.9.

[11]. Стасюк О.І. Базові характеристики та класифікація кризових ситуацій в ІТ-сфері / О.І. Стасюк, А.І. Гізун // Інфокомунікації – сучасність та майбутнє: Всеукр. наук.-практ. конф. 6-7 жовтня 2011 р. : тези доп. – Одеса: ОНАЗ, 2011. – С. 62-65.

[12]. Гізун А.І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. – 2013. –№1 (58). – С.66-75.

[13]. Луцкий М.Г. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцький, А.В. Гавриленко, А.А. Корченко, А.А. Охрименко // Захист інформації. – 2012. – №2 (55). – С. 5-13

[14]. EM-DAT: The OFDA/CRED International Disaster Database [Електронний ресурс] / UCL - Brussels, Belgium. – Режим доступу: http: //www.em-dat.net

[15]. Guha-Sapir D. Annual Disaster Statistical Review 2010 [Електронний ресурс] / Debby Guha-Sapir, Femke Vos, Regina Below, Sylvain Ponserre // Centre for Research on the Epidemiology of Disasters (CRED). – Режим доступу: http://www.cred.be/ sites/default/files/ADSR_2010.pdf.

[16]. Корченко О. Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / О. Г. Корченко. - К. : МК-Пресс, 2006. - 320 с.

[17]. Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. - 2012. - №2 (55) . - С. 47-51

REFERENCES

[1]. Petrenko S. A.,Belyaev A. V.Business management continuity. Your business will be continuing, S. A. Petrenko,A. V. Belyaev, M.: DMKPress, IT Company, 2011, 400 p.

[2]. VanBonJan. IT Service and Management. Elementary cource ITIL, JanVanBon, Van Haren Publishing, by ITSMF Netherlands, 2003, 72 p.
[3]. HarrisS. CISSP Certification All-in-One Exam Guide, 5th edition, Mc Graw-Hill Osborne Media, 2010, 1216 p.
[4]. Business continuity management. Code of practice: BS25999-1:2006, BSI British Standards, 2006, 28 p.
[5]. Business continuity management. Specification: BS25999-2:2007, BSI British Standards, 2007, 38 p.
[6]. Singapore Standard for Business Continuity Management: SS540:2008, SPRING Singapore, 2008, 54 p.
[7]. Business continuity – Managing disruption-related risk: AS/NZS 5050 – Standards Australia, 2010, 53 p.
[8]. Gudkova D. Kaspersky Security Bulletin. Spam in year 2013 [Electronic resource]: article / D.Gudkova., Mode of access: http://www.securelist.com/ru/ analysis/208050828/Kaspersky_Security_Bulletin_Spam_v_2013_godu
[9]. Garnaeva M., Kaspersky Security Bulletin 2013. Main Statictics of the year 2013 [Electronic resource]: article / Mariya Garnaeva, Kristian Phunk – Mode of access: https://www.securelist.com/ru/analysis/208050822/Kaspersky_Security_Bulletin_2013_Osnovnaya_statistika_za_2013_god
[10]. Gizun A. I. Current approaches to protecting information resources for business continuity, A. I. Gizun, V. O. Gnatuk, O. P. Duksenko, A. O. Korchenko, Materials of the 10thscience – technical conferention «AVIA-2011», K.: NAU, 2011, T1, P. 2.5-2.9.
[11]. Stasyuk O.I. The baseline characteristics and classification of crises in the IT field, O.I. Stasyuk, A.I. Gizun, Infocommunications - Presentand Future: International Ukraine Conference. October, 6 – 7, 2011 p. :report thesis, Odesa: ONAZ, 2011, P. 62-65.
[12]. Gizun A.I. The main parameters to identify the offending information security, A.I. Gizun, V.V. Voluans`ka, V.O. Ryndyuk, S. O. Gnatyk, Information security, 2013, №1 (58), P. 66-75.
[13]. Lutskiy M.G. Model standards of linguistic variables for systems detect attacks, M.G. Lutskiy, A.V. Gavrelenko, A.A. Korchenko, A.A. Okhrimenko, Information security, 2012, №2 (55), P. 5-13.
[14]. EM-DAT: The OFDA/CRED International Disaster Database [Electronic resource], UCL - Brussels, Belgium, Mode of access: http: //www.em-dat.net
[15]. Guha-Sapir D. Annual Disaster Statistical Review 2010 [Electronic resource], Debby Guha-Sapir, FemkeVos, Regina Below, Sylvain Ponserre, Centre for Research on the Epidemiology of Disasters (CRED), Mode of access: http://www.cred.be/sites/default/files/ADSR_2010.pdf.
[16]. Korchenko O.G. Building security systems on fuzzy sets [Text] : theory and practical solutions, O.G. Korchenko, K. : MK-Press, 2006, 320 p.
[17]. Stasiuk A.I. The basic model parameters to build systems detect attacks, A.I. Stasiuk, A.A. Korchenko, Information security, 2012, № 2 (55),- P. 47-51.

ПАРАМЕТРИ ПРОГНОЗУВАННЯ І ІДЕНТИФІКАЦІЇ АТАК В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Питання, пов'язані з прогнозуванням, моніторингом та виявленням кризових ситуацій в інформаційно-комунікаційних системах мають велике наукове і практичне значення. У концепції управління безперервністю бізнесу ці процеси займають центральні позиції, визначаючи можливості всіх використовуваних механізмів у сфері відновлення бізнес-процесів і захисту інформаційних ресурсів в умовах впливу кризових ситуацій. Будь-яка кризова ситуація є наслідком множини інцидентів або атак. Виходячи з цього визначення і формалізація основних параметрів, які можуть бути використані для виявлення та ідентифікації комп'ютерних атак, безумовно є актуальним завданням. Саме цим питанням присвячено це дослідження. Так, чітке визначення множини параметрів, що знімаються як на мережевому, так і локальному рівні, дозволить враховувати особливості кожної кризової ситуації, атаки або інциденту і, як наслідок, підвищити ефективність систем захисту та превентивних засобів. Основні результати роботи можуть бути використані для побудови системи прогнозування, виявлення та ідентифікації комп'ютерних атак в інформаційно-комунікаційних системах на базі методів нечіткої логіки.

Ключові слова: кризова ситуація, ідентифікація кризових ситуацій, інформаційно-комунікаційна система, нечітка логіка, кортеж, параметр, управління безперервністю бізнесу, інформаційні ресурси, комп'ютерні атаки.

PARAMETERS IDENTIFICATION AND PREDICTION OF ATTACKS IN THE INFORMATION AND COMMUNICATION SYSTEM

Issues related to the prediction, monitoring and detection of critical situations in the information and communication systems, are of great scientific and practical importance. These processes occupy central positions in the concept of business continuity management, defining the capabilities of all the mechanisms use dint here assumption of business processes and the protection of information resources under the conditions of crisis situations. Any crisis is a consequence of the aggregate incidents or attacks. Based on this definition and formalization of the main parameters that can be used for detection and identification of cyber attacks are certainly an urgent task. This study is devoted to these issues. Thus, a clear definition of a set of parameters, as filmed on a network and local level, will allow to take into account the particularities of each crisis, attack or information security incident and, as a consequence, increase the effectiveness of preventive protection systems and equipment. The main results can be used to construct a system for forecasting, detection and identification of computer attacks in the information and communication systems based on fuzzy logic methods.

Keywords: crisis, identity crises, information and communication system, fuzzy logic, cortege, parameter, business continuity management, information resources, cyber attacks.

Азарсков Валерій Миколайович, доктор технічних наук, професор, завідувач кафедри систем управління літальних апаратів Національного авіаційного університету.
E-mail: azarskov@nau.edu.ua
Азарсков Валерий Николаевич, доктор технических наук, профессор, заведующий каферой систем управления летальных аппаратов Национального авиационного университета.
Azarskov Valeriy, Doctor of Engineering Science, Professor, head of Academic Department of Aircraft Control Systems, National Aviation University.

Гізун Андрій Іванович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: andriy.gizun@gmail.com
Гизун Андрей Иванович, ассистент кафедры безопасности информационных технологий Национального авиационного университета.
Gizun Andrii, Assistant of Academic Department of IT-security, National Aviation University.
Грехов Андрій Михайлович, доктор фізико-математичних наук, професор, професор кафедри аеронавігаційних систем Національного авіаційного університету.
E-mail: grekhovam@ukr.net
Грехов Андрей Михайлович, доктор физико-математических наук, профессор, профессор кафедры аэронавигационных систем Национального авиационного университета.
Grekhov Andrii, Doctor of Physical and Mathematical Sciences, Professor, Professor of Academic Department of Air Navigation Systems, National Aviation University.

Скворцов Сергій Олександрович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: ssamailer@gmail.com
Скворцов Сергей Александрович, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Skvortsov Sergiy, PhD, Associate Professor of the Academic Department of IT-security, National Aviation University.