УДК 519.862

Т.В.Глотова, Х.И.Бешер

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Воронежский институт высоких технологий

Статья посвящена анализу особенностей информационной безопасности распределенных систем. Указаны причины формирования систем. Рассмотрены основные составляющие информационной безопасности компьютерных систем. Обсуждаются мотивы совершения компьютерных преступлений. Дана классификация каналов несанкционированного доступа. Приведены уровни создания режимов информационной безопасности. Даны принципы формирования надежной защиты системы. Указано, каким образом осуществляется выбор информации, на базе которой происходят процедуры по идентификации и аутентификации пользователей. Отмечается тенденция опережающего развития, касающегося применения биометрических систем идентификации.

Ключевые слова: информационная безопасность, система, компьютер, информация, пользователь, защита.

Распределенная система - совокупность независимых компьютеров, которая представляется пользователю единым компьютером [1-4]. Примеры: сети рабочих станций (проведение выбора процессоров для исполнения программ, единые файловые системы), роботизированные заводы (роботы являются связанными с разными компьютерами, но функционируют таким же образом, как и внешние устройства в едином компьютере, банки, имеющие множество филиалов, системы, позволяющие резервировать авиабилеты.

Причины создания распределенных систем следующие [5-8]:

1-я причина - экономическая. Закон Гроша (Herb Grosh) - быстродействие процессора пропорциональна квадрату его стоимости. С появлением микропроцессоров закон перестал действовать - за двойную цену можно получить тот же процессор с несколько большей частотой.

2-я причина - можно достичь такой высокой производительности путем объединения микропроцессоров, которая недостижима в централизованном компьютере.

3-я причина - естественная распределенность (банк, поддержка совместной работы группы пользователей).

4-я причина - надежность (выход из строя нескольких узлов незначительно снизит производительность).

5-я причина - наращиваемость производительности. В будущем главной причиной будет наличие огромного количества персональных компьютеров и необходимость совместной работы без ощущения неудобства от географического и физического распределения людей, данных и машин.

Причины объединения рабочих станций в сети [9-13]:

1. Необходимость разделять данные.
2. Преимущество разделения дорогих периферийных устройств, уникальных информационных и программных ресурсов.
3. Достижение развитых коммуникаций между людьми. Электронная почта во многих случаях удобнее писем, телефонов и факсов.
4. Гибкость использования различных ЭВМ, распределение нагрузки.
5. Упрощение постепенной модернизации посредством замены компьютеров.

Недостатки распределенных систем:

1. Проблемы ПО (приложения, языки, ОС).
2. Проблемы коммуникационной сети (потери информации, перегрузка, развитие и замена).

Быстро появляющиеся новые компьютерные информационные технологии определяют большие изменения в нашей жизни [14-18]. Об информации можно говорить как о товаре, который мы можем приобретать, продавать, обменивать. Можно отметить, что стоимость информации во многих случаях в тысячи раз превышает стоимость компьютерных систем, в которых она хранится.

От того, какая безопасность информационных технологий в существующих условиях мы можем предсказать здоровье, а иногда и жизнь многих людей. Это связано с усложнением и повсеместным распространением автоматизированных систем, связанных с обработкой информации.

Информационная безопасность показывает степень защищенности информационных систем от случайных или преднамеренных вмешательств, наносящих ущерб для владельцев или пользователей информации.

В практических случаях весьма важными можно считать три составляющих информационной безопасности:

- характеристики доступности (возможности в течение разумного времени получать требуемые информационные услуги);
- характеристики целостности (информация должна быть актуальна и непротиворечива, стремятся к ее защищенности от разрушающих воздействий и несанкционированных изменений);
- характеристики конфиденциальности (обеспечение защиты от несанкционированного чтения).

Когда нарушается доступность, целостность и конфиденциальность информации, то это может быть связано с разными влияниями, которым подвергаются компьютерные информационные системы.

Если говорить о современной информационной системе, то она является сложной системой, которая содержит большое число составляющих, имеющих разную величину автономности, они характеризуются взаимными связями, между ними имеется обмен данных [19-22]. Существуют различные алгоритмы по обработке данных [23-25]. На практике любые компоненты могут подвергаться внешним воздействиям или выходить из строя [26, 27]. Мы можем осуществить разбиение компонентов автоматизированных информационных систем на такие виды:

- аппаратные средства – в них входят компьютеры, а также те детали, из которых они собраны (процессор, монитор, терминал, периферийные устройства - дисковод, принтер, контроллер, кабель, линии связи и др.);
- программы – они могут быть различными – программы внешних производителей, исходные коды, объектный код, загрузочный модуль; операционная система и системная программа (компилятор, компоновщик и т.д.), утилита, диагностическая программа и т.д.;
- данные – они могут храниться временным образом и постоянным, с применением магнитных носителей, в печатном виде, архивы, системный журнал и др.;
- персонал.

Можно сделать разделение опасных воздействий на компьютерные информационные системы как случайные и преднамеренные. Исходя из анализа существующих концепций, базирующихся на проектировании, формировании и эксплуатации информационных систем, мы можем говорить о том, что информация связана с разными случайными воздействиями по всем этапам жизненных циклов систем. В качестве причин случайных воздействий, которые появляются в эксплуатационных условиях, можно отметить:

- появление аварийных ситуаций вследствие того, что происходят стихийные бедствия и отключения электропитания;
- возникновение отказов и сбоев в аппаратуре;
- появление ошибок в программном обеспечении;
- появление ошибок при функционировании персонала;
- возникновение помех в линиях связи вследствие того, что оказывает воздействие внешняя среда.

Преднамеренные воздействия определяются целенаправленными действиями нарушителей. В качестве нарушителей могут быть служащие, посетители, конкуренты, наемники. Действия нарушителей связаны с самыми различными мотивами:

- недовольство служащих своей карьерой;
- взятками;
- возникновением любопытства;
- появлением конкурентной борьбы;
- за счет стремления получить самоутверждение любой ценой.

Есть возможности для того, чтобы сформировать характеристики гипотетической модели потенциальных нарушителей [28-30]:

- квалификация нарушителей на уровнях разработчиков такой системы;
- в качестве нарушителя могут выступать как посторонние лица, так и законные пользователи систем;
- нарушители обладают информацией о том, каковы принципы функционирования систем;
- нарушители выбирают самые слабые звенья в защите.

Достаточно распространенными и многообразными видами компьютерных нарушений являются типы несанкционированного доступа (НСД). НСД может использовать любые ошибки в системах защиты и появляется, когда будет нерациональный выбор средств защиты, их некорректная установка и настройка.

Проведем классификацию каналов НСД, по которым можно осуществить хищение, изменение или уничтожение информации:

- Через человека:
  - хищение носителей информации;
  - чтение информации с экрана или клавиатуры;
  - чтение информации из распечатки.
- Через программу:
  - перехват паролей;
  - расшифровка зашифрованной информации;
  - копирование информации с носителя.
- Через аппаратуру:
  - подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
  - перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основные особенности любых компьютерных сетей заключаются в том, что их составляющие являются распределенными в пространстве. Связи между узлами в сетях достигаются физическим образом на основе сетевых линий и программным образом на базе механизмов сообщений. В таком описании передача управляющих сообщений и данных, пересылаемых между узлами сетей, осуществляется как пакеты обмена. Компьютерная сеть характерна тем, что против нее

совершаются различные виды удаленных атак. Нарушители могут быть за тысячи километров от атакуемых объектов, при этом нападения могут быть не только на конкретные компьютеры, но и на информацию, которая передается по сетевому каналу связи.

Создание режимов информационной безопасности – является комплексной проблемой. Меры для того, чтобы достичь ее решения мы можем разделить по нескольким уровням:

- законодательные (закон, нормативный акт, стандарт и т.п.);
- морально-этические (разные нормы поведения, и если их не соблюдать, то это приводит к тому, что падает престиж конкретных людей или целых организаций);
- административные (действия, связанные с общим характером, которые осуществляются руководством организаций);
- физические (механическое, электро- и электронно-механическое препятствие по возможным путям проникновения возможных нарушителей);
- аппаратно-программные (электронное устройство и специальная программа защиты информации).

Использование единой совокупности всех подобных мер, которые направлены на то, чтобы противодействовать угрозам безопасности с целями минимизации возможностей ущерба, дают системную защиту.

Чтобы система защиты была надежной, для нее должны выполняться следующие принципы:

- Величина стоимости средств, предназначенных для обеспечения защиты должна быть меньше, по сравнению с размерами возможных ущербов.
- Для каждого из пользователей должны быть предусмотрены минимальные наборы привилегий, необходимых для работы.
- Защита будет более эффективной, если для пользователей будет упрощаться работа с ней.
- Возможности отключения для экстренных случаев.
- Специалисты, которые связаны с системами защиты, должны в полной мере понимать каковы принципы ее работы и в случаях появления затруднительной ситуации адекватным образом на нее реагировать.
- Всю систему обработки информации необходимо защищать.
- Разработчиками систем защиты, не должны теми, кого такие системы будут контролировать.
- Системы защиты должны осуществлять вывод доказательств своей корректной работы.

- Необходимо, чтобы для людей, которые занимаются вопросами обеспечения информационной безопасности, была предусмотрена личная ответственность.
- Для объектов защиты следует осуществлять подразделение на группы таким образом, чтобы при нарушении защиты в одних группах это не оказывало влияние на степень безопасности других.
- Надежные системы защиты должны быть полностью протестированы и согласованы.
- Защита будет более эффективная и гибкая, если ею допускаются изменения в параметрах со стороны администраторов.
- Системы защиты должны разрабатываться, базируясь на предположениях, что пользователь будет совершать грубые ошибки и, имеет плохие намерения.
- Весьма важное и критическое решение должно приниматься людьми.
- То, что механизмы защиты существуют необходимо, по возможности, скрывать от пользователей, функционирование которых происходит под контролем.

Систему идентификации и аутентификации пользователя применяют для того, чтобы ограничить доступ случайного и незаконного пользователя к ресурсам компьютерных систем. Основы общего алгоритма работы подобных систем состоят в том, чтобы получать от пользователей информацию, которая будет удостоверять их личность, проверять ее подлинность и потом предоставлять (или не предоставлять) таким пользователям возможности для работы с этой системой.

При формировании подобных систем появляются проблемы, связанные с выбором информации, на базе которой происходят процедуры по идентификации и аутентификации пользователей. Мы можем отметить такие виды:

- секретная информация, ее имеют пользователи (пароли, секретные ключи, персональные идентификаторы и т.п.); пользователи должны запомнить такую информацию или применять специальные средства, чтобы ее хранить;
- физиологический параметр человека (отпечаток пальца, рисунки радужной оболочки глаз и т.п.) или особенности, связанные с поведением (характеристики работы на клавиатурах и т.п.).

Системы, базирующиеся на первых видах информации, рассматриваются как традиционные. Системы, применяющие второй вид информации, называются биометрические. Необходимо сказать, что в

последнее время биометрические системы идентификации применяются во многих практических приложениях.

ЛИТЕРАТУРА

1. Глотова Т.В. Особенности архитектуры защищенного корпоративного портала / Т.В.Глотова, В.Н.Кострова / Вестник Воронежского института высоких технологий. 2016. № 16. С. 29-32.
2. Лавлинская О.Ю. Технологии облачных вычислений и их применение в решении практических задач / О.Ю.Лавлинская, Т.М.Янкис // Вестник Воронежского института высоких технологий. 2016. № 16. С. 33-36.
3. Часовской А.А. Оценка перспектив внедрения облачных вычислений на предприятиях и в государственном секторе на примере ФРГ / А.А.Часовской, Е.В.Алференко / Вестник Воронежского института высоких технологий. 2016. № 16. С. 94-97.
4. Баранов А.В. Проблемы функционирования mesh-сетей / А.В.Баранов // Вестник Воронежского института высоких технологий. 2012. № 9. С. 49-50.
5. Сазонова С.А. Оценка надежности работы сетевых объектов / С.А.Сазонова // Вестник Воронежского института высоких технологий. 2016. № 16. С. 40-42.
6. Нечаева А.И. Особенности функционирования информационных баз на складе / А.И.Нечаева // Вестник Воронежского института высоких технологий. 2016. № 16. С. 64-66.
7. Канавин С.В. Перспективы применения систем мобильного широкополосного доступа в сетях подвижной радиосвязи на основе стандартов MOBILE WIMAX и LTE / С.В.Канавин, А.С.Лукьянов // Вестник Воронежского института высоких технологий. 2016. № 16. С. 79-82.
8. Мельникова Т.В. Модель проектирования беспроводных систем связи с учетом природных и промышленных помех / Т.В.Мельникова // Вестник Воронежского института высоких технологий. 2016. № 16. С. 61-63.
9. Подсистема проектирования защищенных беспроводных сетей / И.Я. Львович, А.П. Преображенский, Е. Ружицкий, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 556-559.
10. Белоножкин В.И. Методика формализации правила разграничения доступа к информационным ресурсам / В.И. Белоножкин, О.Н. Чопоров // Информация и безопасность. - 2007. - Т. 10. - № 1. - С. 169-172.
11. Малышев В.А. Структурная модель подсистемы решения задач и прогнозирования в системах автоматизированного проектирования /

В.А.Малышев // Вестник Воронежского государственного технического университета. 2005. Т. 1. № 11.

12. Литвинский К.О. Модель подсистемы поддержки принятия решения в системе управления техногенными рисками предприятиях топливно-энергетического комплекса / К.О.Литвинский, В.А.Малышев, Ю.В.Никитенко // Экономика устойчивого развития. 2015. № 1 (21). С. 91-100.
13. Малышев В.А. Нечеткие алгоритмы планирования и модели взвешенного прогноза распределения ресурсов системы управления специального назначения / В.А.Малышев, В.С.Прокофьев // Вестник Воронежского института высоких технологий. 2008. № 3. С. 049-052.
14. Преображенский Ю.П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 116-119.
15. Паневин Р.Ю. Структурные и функцинальные требования к программному комплексу представления знаний / Р.Ю.Паневин, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2008. № 3. С. 061-064.
16. Паневин Р.Ю. Реализация транслятора имитационно-семантического моделирования / Р.Ю.Паневин, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 057-060.
17. Чопоров О.Н. Рационализация управления региональными системами на основе использования методов системного анализа, информационных и ГИС-технологий / О.Н.Чопоров, Н.А.Гладских, С.С.Пронин, М.И.Чудинов, С.Н.Семенов, К.Л.Матюшевский // Прикладные информационные аспекты медицины. 2007. Т. 10. № 2. С. 15-19.
18. Формирование требований к системе информационной безопасности в проектных организациях нефтегазового комплекса / Б.В. Васильев, Н.И. Баранников, А.В. Заряев, В.С. Зарубин, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 508-511.
19. Применение каскадных моделей при оценке рисков распространения вредоносной информации в социальных сетях / Д.О. Карпеев, Д.А. Савинов, А.В. Заряев, В.С. Зарубин, О.Н. Чопоров // Информация и безопасность. - 2015. - Т. 18. - № 4. - С. 512-515.
20. Львович Я.Е. Адаптивное управление марковскими процессами в конфликтной ситуации / Я.Е.Львович, Ю.П.Преображенский, Р.Ю.Паневин // Вестник Воронежского государственного технического университета. 2008. Т. 4. № 11. С. 170-171.
21. Воронов А.А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А.А.Воронов,

И.Я.Львович, Ю.П.Преображенский, В.А.Воронов // Информация и безопасность. 2006. Т. 9. № 2. С. 8-11.
22. Зяблов Е.Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е.Л.Зяблов, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2009. № 5. С. 024-026.
23. Иванов М.С. Разработка алгоритма отсечения деревьев / М.С.Иванов, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2008. № 3. С. 031-032.
24. Ермолова В.В. Архитектура системы обмена сообщений в немаршрутизируемой сети / В.В.Ермолова, Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2010. № 7. С. 79-81.
25. Преображенский Ю.П. Адаптивные алгоритмы для бесконечных стохастических игр / Ю.П.Преображенский // Вестник Воронежского института высоких технологий. 2010. № 7. С. 46-47.
26. Исследование устойчивости беспроводных сетей в условиях блокирования сигнала / И.Я. Львович, О.Н. Чопоров, А.П. Преображенский, В.Б. Щербаков // Информация и безопасность. - 2016. - Т. 19. - № 2. - С. 254-257.
27. DDOS-Атаки на распределнные автоматизированные системы: управление риском при нерегулярном распределении ущерба / Е.А. Попов, О.Н. Чопоров, Л.Г. Попова, О.А. Остапенко // Информация и безопасность. - 2014. - Т. 17. - № 4. - С. 630-633.
28. Спам-атаки на распределнные автоматизированные системы: аналитическое выражение ущерба / Е.А. Попов, О.Н. Чопоров, Л.Г. Попова, О.А. Остапенко // Информация и безопасность. - 2014. - Т. 17. - № 4. - С. 634-637.

T.V. Glotova, H.I.Besher

THE FEATURES OF INFORMATION SECURITY DISTRIBUTED SYSTEMS

Voronezh Institute of high technologies

The paper is devoted to analysis of peculiarities of information security in distributed systems. It states the reasons for the formation of systems. The basic components of information security of computer systems are given. The motives of committing computer crimes are discussed. A classification of channels of unauthorized access is shown. The levels of creation of regimes of information security are concretized. The principles form a reliable protection system are given. It Specified how the system selects information on the basis of which there procedures for identification and authentication of users. There is a trend of advanced development for the use of biometric identification systems.

Keywords: information security, system, computer, information, user, protection.

REFERENCES

1. Glotova T.V. Osobennosti arkhitektury zashchishchennogo korporativnogo portala / T.V.Glotova, V.N.Kostrova / Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 29-32.
2. Lavlinskaya O.Yu. Tekhnologii oblachnykh vychisleniy i ikh primenenie v reshenii prakticheskikh zadach / O.Yu.Lavlinskaya, T.M.Yankis // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 33-36.
3. Chasovskoy A.A. Otsenka perspektiv vnedreniya oblachnykh vychisleniy na predpriyatiyakh i v gosudarstvennom sektore na primere FRG / A.A.Chasovskoy, E.V.Alferenko / Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 94-97.
4. Baranov A.V. Problemy funktsionirovaniya mesh-setey / A.V.Baranov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2012. No.9. pp. 49-50.
5. Sazonova S.A. Otsenka nadezhnosti raboty setevykh ob''ektov / S.A.Sazonova // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 40-42.
6. Nechaeva A.I. Osobennosti funktsionirovaniya informatsionnykh baz na sklade / A.I.Nechaeva // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 64-66.
7. Kanavin S.V. Perspektivy primeneniya sistem mobil'nogo shirokopolosnogo dostupa v setyakh podvizhnoy radiosvyazi na osnove standartov MOBILE WIMAX i LTE / S.V.Kanavin, A.S.Luk'yanov // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 79-82.
8. Mel'nikova T.V. Model' proektirovaniya besprovodnykh sistem svyazi s uchetom prirodnykh i promyshlennykh pomekh / T.V.Mel'nikova // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2016. No.16. pp. 61-63.
9. Podsistema proektirovaniya zashchishchennykh besprovodnykh setey / I.Ya. L'vovich, A.P. Preobrazhenskiy, E. Ruzhitskiy, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 556-559.
10. Belonozhkin V.I. Metodika formalizatsii pravila razgranicheniya dostupa k informatsionnym resursam / V.I. Belonozhkin, O.N. Choporov // Informatsiya i bezopasnost'. - 2007. - Vol. 10. - No.1. - pp. 169-172.
11. Malyshev V.A. Strukturnaya model' podsistemy resheniya zadach i prognozirovaniya v sistemakh avtomatizirovannogo proektirovaniya / V.A.Malyshev // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2005. Vol. 1. No.11.
12. Litvinskiy K.O. Model' podsistemy podderzhki prinyatiya resheniya v sisteme upravleniya tekhnogennymi riskami predpriyatiyakh toplivno-energeticheskogo kompleksa / K.O.Litvinskiy, V.A.Malyshev,

Yu.V.Nikitenko // Ekonomika ustoychivogo razvitiya. 2015. No.1 (21). pp. 91-100.

13. Malyshev V.A. Nechetkie algoritmy planirovaniya i modeli vzveshennogo prognoza raspredeleniya resursov sistemy upravleniya spetsial'nogo naznacheniya / V.A.Malyshev, V.S.Prokof'ev // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 049-052.
14. Preobrazhenskiy Yu.P. Otsenka effektivnosti primeneniya sistemy intellektual'noy podderzhki prinyatiya resheniy / Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 116-119.
15. Panevin R.Yu. Strukturnye i funktsinal'nye trebovaniya k programmnomu kompleksu predstavleniya znaniy / R.Yu.Panevin, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 061-064.
16. Panevin R.Yu. Realizatsiya translyatora imitatsionno-semanticheskogo modelirovaniya / R.Yu.Panevin, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 057-060.
17. Choporov O.N. Ratsionalizatsiya upravleniya regional'nymi sistemami na osnove ispol'zovaniya metodov sistemnogo analiza, informatsionnykh i GIS-tekhnologiy / O.N.Choporov, N.A.Gladskikh, S.S.Pronin, M.I.Chudinov, S.N.Semenov, K.L.Matyushevskiy // Prikladnye informatsionnye aspekty meditsiny. 2007. Vol. 10. No.2. pp. 15-19.
18. Formirovanie trebovaniy k sisteme informatsionnoy bezopasnosti v proektnykh organizatsiyakh neftegazovogo kompleksa / B.V. Vasil'ev, N.I. Barannikov, A.V. Zaryaev, V.S. Zarubin, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 508-511.
19. Primenenie kaskadnykh modeley pri otsenke riskov rasprostraneniya vredonosnoy informatsii v sotsial'nykh setyakh / D.O. Karpeev, D.A. Savinov, A.V. Zaryaev, V.S. Zarubin, O.N. Choporov // Informatsiya i bezopasnost'. - 2015. - Vol. 18. - No.4. - pp. 512-515.
20. L'vovich Ya.E. Adaptivnoe upravlenie markovskimi protsessami v konfliktnoy situatsii / Ya.E.L'vovich, Yu.P.Preobrazhenskiy, R.Yu.Panevin // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2008. Vol. 4. No.11. pp. 170-171.
21. Voronov A.A. Obespechenie sistemy upravleniya riskami pri vozniknovenii ugroz informatsionnoy bezopasnosti / A.A.Voronov, I.Ya.L'vovich, Yu.P.Preobrazhenskiy, V.A.Voronov // Informatsiya i bezopasnost'. 2006. Vol. 9. No.2. pp. 8-11.
22. Zyablov E.L. Razrabotka lingvisticheskikh sredstv intellektual'noy podderzhki na osnove imitatsionno-semanticheskogo modelirovaniya / E.L.Zyablov, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2009. No.5. pp. 024-026.

23. Ivanov M.S. Razrabotka algoritma otsecheniya derev'ev / M.S.Ivanov, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2008. No.3. pp. 031-032.
24. Ermolova V.V. Arkhitektura sistemy obmena soobshcheniy v nemarshrutiziruemoy seti / V.V.Ermolova, Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2010. No.7. pp. 79-81.
25. Preobrazhenskiy Yu.P. Adaptivnye algoritmy dlya beskonechnykh stokhasticheskikh igr / Yu.P.Preobrazhenskiy // Vestnik Voronezhskogo instituta vysokikh tekhnologiy. 2010. No.7. pp. 46-47.
26. Issledovanie ustoychivosti besprovodnykh setey v usloviyakh blokirovaniya signala / I.Ya. L'vovich, O.N. Choporov, A.P. Preobrazhenskiy, V.B. Shcherbakov // Informatsiya i bezopasnost'. - 2016. - Vol. 19. - No.2. - pp. 254-257.
27. DDOS-Ataki na raspredelnnye avtomatizirovannye sistemy: upravlenie riskom pri neregulyarnom raspredelenii ushcherba / E.A. Popov, O.N. Choporov, L.G. Popova, O.A. Ostapenko // Informatsiya i bezopasnost'. - 2014. - Vol. 17. - No.4. - pp. 630-633.
28. Spam-ataki na raspredelnnye avtomatizirovannye sistemy: analiticheskoe vyrazhenie ushcherba / E.A. Popov, O.N. Choporov, L.G. Popova, O.A. Ostapenko // Informatsiya i bezopasnost'. - 2014. - Vol. 17. - No.4. - pp. 634-637.