характеризується структурною кризою, адекватною формою рішення якої є структурна перебудова системи.

Час перебудови інформаційної системи $t_{пер}$ характеризується особливостями її структури, стабільність якої до різних впливів характеризується кількістю, спрямованістю й вагою зв'язків між її компонентами.

Визначення часу, наявного в інформаційної системи на структурну перебудову, здійснюється шляхом прогнозування можливого підвищення системи. Метод прогнозування полягає в тому, щоб оцінити, чи встигає система відреагувати на множину зовнішніх впливів за час $t$, характерна для даної структури, чи ні. Якщо не встигає, то необхідно змінити свою структуру, якщо в ній бракує елементів зв'язків, необхідних для такого блокування.

Викладене дозволить сформулювати істотні, необхідні й стійкі (повторювані) відносини, що виникають у процесі інформаційного впливу інформаційних систем.

Інформаційна система може перебувати в стані оптимального функціонування тільки протягом обмеженого часу $t$. Цей стан характеризується блокуванням усіх каналів інформаційного впливу й через час $t + \Delta t$ у чинність свого існування перейде в стан, при якому виникають нові канали. Зворотний перехід можливий тільки в результаті структурної перебудови системи.

Впровадження ЗПІВ у ПТС інформаційної системи є одним з видів взаємодії інформаційних систем.

Інформаційна взаємодія інформаційних систем являє собою систему, межі якої визначаються глибиною структурних зв'язків між її компонентами, які характеризуються мовними аспектами динамічної форми існування системи.

**Список літератури**

1. Коженеський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. - Термінологічний довідник з питань технічного захисту інформації/ За ред. проф. В.О. Хорошка, вид.4-е, доповнене й перероб. - К.: Вид. ДУІКТ, 2007.-365с.
2. Браіловський М.М., Головань С.М. та інші. – Технічний захист інформації на об'єктах інформаційної діяльності/ За ред.проф. В.О. Хорошка. – К.: Вид. ДУІКТ, 2007. – 178с.
3. Расторгуев С.П. Инфицирование как способ защиты жизни. Вирусы: биологические, социальные, психические, компьютерные. – М.: Яхтсмен, 1996. – 121с.
4. Азаров С.С., Хорошко В.А. – Современные методы провайдинга. – К.: ПолиграфКонсалтинг, 2006. - 98с.
5. Волобуев С.В. к вопросу об информационном взаимодействии систем // Вопросы защиты информации, № 4, 2002. – с.2-7.

*Надійшла 18.03.2008р.*

УДК 65.012.8/342.738(477)

С.Л.Емельянов

## НЕКОТОРЫЕ ВИДЫ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОРУЖИЯ

***Постановка проблемы.*** Согласно прогнозам XXI столетие станет веком глобальной информатизации и компьютеризации всего мира и переходом человечества к новому информационному обществу, в котором решающая роль отводится информации,

информационым системам (ИС), информационным ресурсам (ИР) и информационно-телекоммуникационным технологиям (ИТТ).

Исходя из стратегического курса Украины на интеграцию в мировой информационный простор, возникает объективная потребность в анализе как положительных, так и отрицательных явлений, сопровождающих широкомасштабное внедрение ИС и ИТТ.

Наряду с традиционными угрозами, существующими в сфере формирования, хранения и распространения ИР, постоянно возрастают угрозы несанкционированного вмешательства в работу ИС не только с целью получения закрытой информации, но и нарушения ее целостности, доступности и уничтожения, дезорганизации информационной системы державы. Специалисты в области информационных технологий едины во мнении, что, как в свое время достижения ядерной физики вызвали опасность ядерной войны, так и широкая информатизация (компьютеризация) стала источником новых угроз обществу, государству и личности. Появились новые термины и явления: «Информационная война», «Информационное оружие», «Информационный терроризм» и др. [1-20].

***Целью исследований*** является анализ сущности современных способов и средств ведения информационных войн, обоснование классификации видов информационного оружия, а также выявление их взаимосвязи с информационной безопасностью государства.

Вышеуказанные ключевые термины прочно вошли в современный обиход с 90–ых годов прошлого столетия, зародившись в недрах военных министерств и ведомств.

***Анализ исследований и публикаций.*** Первоначально Томас Рона использовал термин «*информационная война*» (ИВ) в отчете, подготовленным им в 1976 г. для компании Boeing, и названный «Системы оружия и информационная война». В отчете отмечалось, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью как в военное, так и в мирное время [3, 4, 10].

Дальнейшее развитие и повсеместное внедрение компьютеризированных ИС и ИТТ, расширение всемирной компьютерной сети Интернет еще более обострили данную проблему, поскольку усилилась зависимость всей системы жизнеобеспечения государства и людей от качества и надежности их функционирования.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих – традиционное пространство и кибѐрпространство, причем последнее имеет даже более важное значение. В число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включена и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут рассматриваться информационная инфраструктура и психика противника («human network») [10].

***Нерешенные проблемы.*** Таким образом, сердцевиной современных ИВ является информация и ее свойства (полнота, адекватность, актуальность, достоверность, избыточность, доступность, объективность и др.), от которых зависит качество принимаемых решений в любой сфере человеческой деятельности. Для достижения информационного превосходства над противником необходимо иметь и развивать различные виды информационного оружия (ИО).

***Изложение основного материала.*** Общепринятого определения ИО в литературе не приводится. На основании» [17]:

«*... информационное оружие – это арсенал средств несанкционированного доступа к информации и выведения из строя электронных систем управления. Информационная «атака» грозит выведением из строя всех электронных систем управления страной, ее вооруженными силами, государственной инфраструктурой и т. д. Разрушатся транспортная и энергетическая (в том числе атомная) системы. Армия и флот будут беспомощны в отражении агрессии. Руководители страны окажутся не в состоянии получать необходимую*

*информацию, принимать и реализовывать какие-либо решения. Использование такого оружия по своим катастрофическим последствиям вполне сопоставимо с применением средств массового поражения».*

По нашему мнению, виды ИО целесообразно классифицировать в зависимости от их потенциальных объектов воздействия, а также на основе способов применения и реализации (рис. 1).

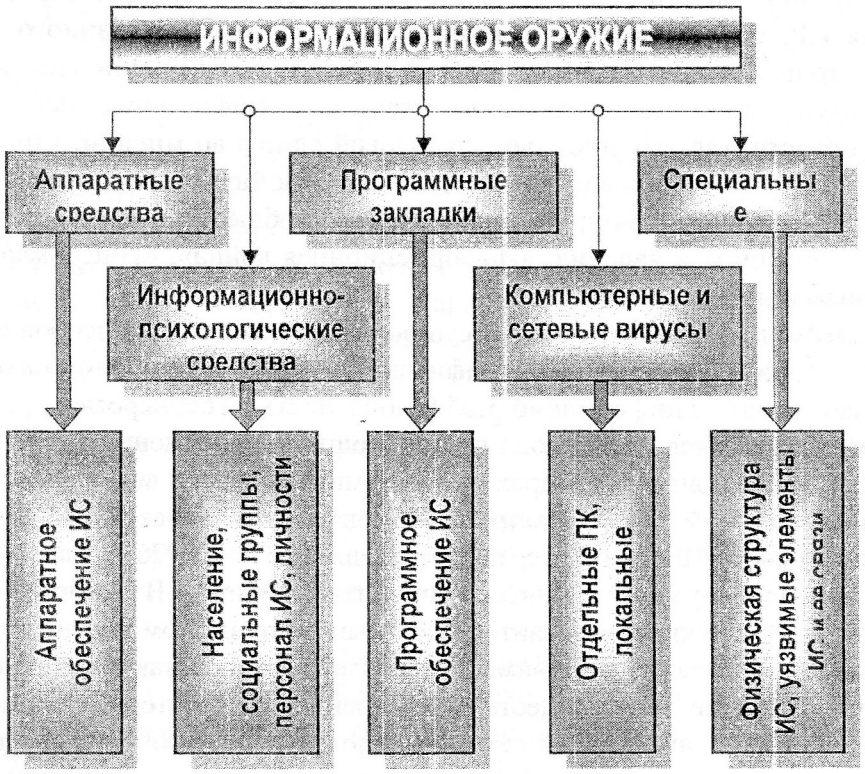



Рис. 1. Базовые виды информационного оружия и объекты его применения

Например, широкое распространение в последние годы получили программное обеспечение (ПО) и аппаратные средства, предназначенные для скрытого слежения за деятельностью пользователей ПК. Данная категория мониторинговых продуктов носит название «программы-шпионы» или «продукты-шпионы» [18].

Согласно недавно опубликованному исследованию компании Websense [15, 16], на компьютерах трети из всех участвовавших в международных проектах в 2004 г. европейских компаний были обнаружены такие шпионские программы («spyware»), позволяющие производить неавторизованный доступ к хранящейся компьютерной информации.

*Программные кейлоггеры* [keyloggers] первоначально предназначались исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (Log-файл), который впоследствии изучался человеком, установившим эту программу. Log-файл может отправляться по сети на сетевой диск, FTP сервер в сети Интернет, по Email и др. В последнее время такие программные продукты выполняют много дополнительных функций – перехват информации из окон, перехват кликов мыши, «фотографирование» экрана и активных окон, ведение учета всех полученных и отправленных Email, мониторинг файловой активности, системного реестра, очереди заданий, отправленных на принтер, перехват звука с микрофона и видеоизображения с веб-камеры, подключенных к компьютеру и др. Примерами известных программных кейлоггеров являются Activity Logger, Ghost Keylogger, HookDump, Invisible KeyLogger Stealth, KeyLog, KeySpy, Perfect Keylogger и др.

*Аппаратные кейлоггеры* [keystroke recording device, hardware keylogger] представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и

компьютером или встроены в саму клавиатуру (см. табл.). Они регистрируют все нажатия клавиш, сделанные на клавиатуре. Процесс регистрации абсолютно невидим для конечного пользователя. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере интересующего объекта, чтобы успешно перехватывать все нажатия клавиш. Объемы внутренней энергонезависимой памяти данных устройств позволяют записывать до 10 миллионов нажатий клавиш.

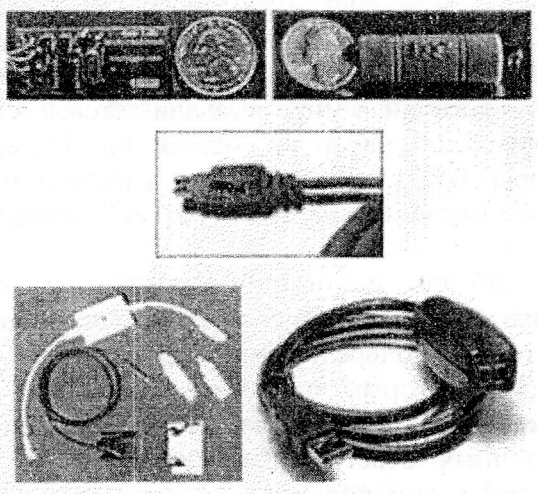
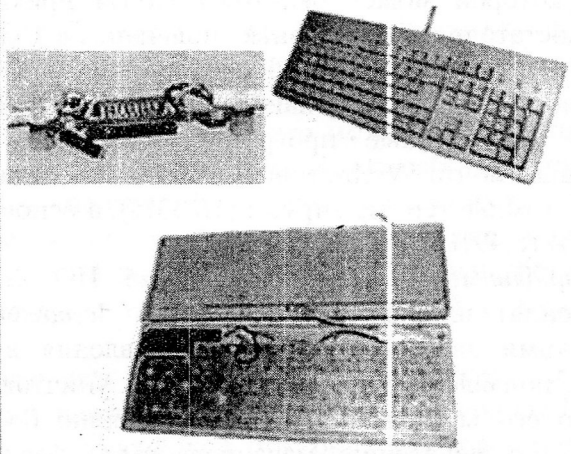
*Программная закладка* (ПЗ) [*program bug*] – несанкционированно внедренная программа (программный модуль), осуществляющая скрытую угрозу информации. Предшественниками ПЗ принято считать троянские программы [6, 19]. «Троянский конь», «троянец» и т. д. представляет собой программу, которая наряду с функциями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению информационной безопасности ИС. Аналогия такой программы с древнегреческим «троянским конем» вполне оправдана, так как в обоих случаях не вызывающая подозрений оболочка таит серьезную угрозу. Опасность «троянского коня» заключается в дополнительном блоке команд, вставленном в исходную безвредную программу, которая затем предоставляется пользователям ИС. Этот блок команд может срабатывать по истечении фиксированного времени, при выполнении определенных логических условий («логическая бомба») или по внешним командам.

Воздействие ПЗ на информацию может иметь разведывательный (перехват и организация скрытых каналов передачи информации), разрушающий (искажение, модификация, уничтожение), а также блокирующий (отказ ИС в обслуживании) характеры, что обусловлено целью враждебного воздействия: нарушение конфиденциальности, целостности или доступности информации (рис. 2).

Сегодня многие угрозы безопасности ИС могут эффективно реализовываться при помощи программных вирусов (ПВ). Такое название они получили за схожесть с биологическими вирусами, в частности, из-за способности к саморазмножению.

Под ПВ понимается автономно функционирующая программа, обладающая способностью к самовключению в тела других программ и последующему самовоспроизведению и самораспространению в компьютерных сетях и отдельных ПК. ПВ разделяют на компьютерные и сетевые вирусы. Последние используют для размножения телекоммуникационные каналы ИС. Принципиальное отличие вируса от троянской программы состоит в том, что после запуска его в ИС он существует самостоятельно (автономно), и в процессе своего функционирования заражает (инфицирует) программы путем включения в них своего текста.

Таблица

| ВНЕШНИЕ АППАРАТНЫЕ КЕЙЛОГГЕРЫ | ВНУТРЕННИЕ АППАРАТНЫЕ КЕЙЛОГГЕРЫ |
|---|---|
|  Современные аппаратные кейлоггеры представляют собой встроенные приспособления, которые выглядят, как оборудование для ПК |  Современный внутренний аппаратный кейлоггер представляет собой встроенное приспособление, которое выглядит, как клавиатура ПК |

**Засновники:** Національний авіаційний університет (КМУЦА)
та Державний університет інформаційно-комунікаційних технологій
Зареєстровано Міністерством інформації України.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 3811 від 10 червня 1999 р.

*Постановою президії ВАК України від 9 червня 1999 р. № 1-05/7 журнал включено* ***до Переліку №1 наукових фахових видань України****,*
*в яких можуть публікуватися результати дисертаційних робіт*
*на здобуття наукових ступенів доктора та кандидата наук в галузі технічних наук*
*(Бюлетень ВАК України, №4, 1999)*



# ЗАХИСТ ІНФОРМАЦІЇ

**№ 3(39) 2008 р.**

Науково-технічний журнал
Засновано у 1999 році
Виходить чотири рази на рік

*Друкується за постановою редакційної колегії журналу*

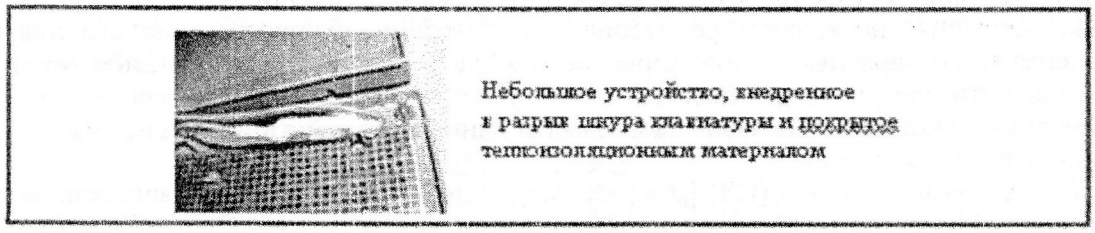
**Видання журналу здійснюється за підтримки фірми "ЕПОС"**



**Адреса редакційної колегії:** 03110 м. Київ-110, вул. Солом'янська, 7, ДУІКТ,
тел. 248-85-79, 248-86-07.

Видавництво ДУІКТ
03110, Київ, вул. Солом'янська, 7.
Надруковано видавництвом ДУІКТ
03110, Київ, вул. Солом'янська, 7.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
Серія ДК №2539 від 26.06.2006 р.

Продолжение таблицы



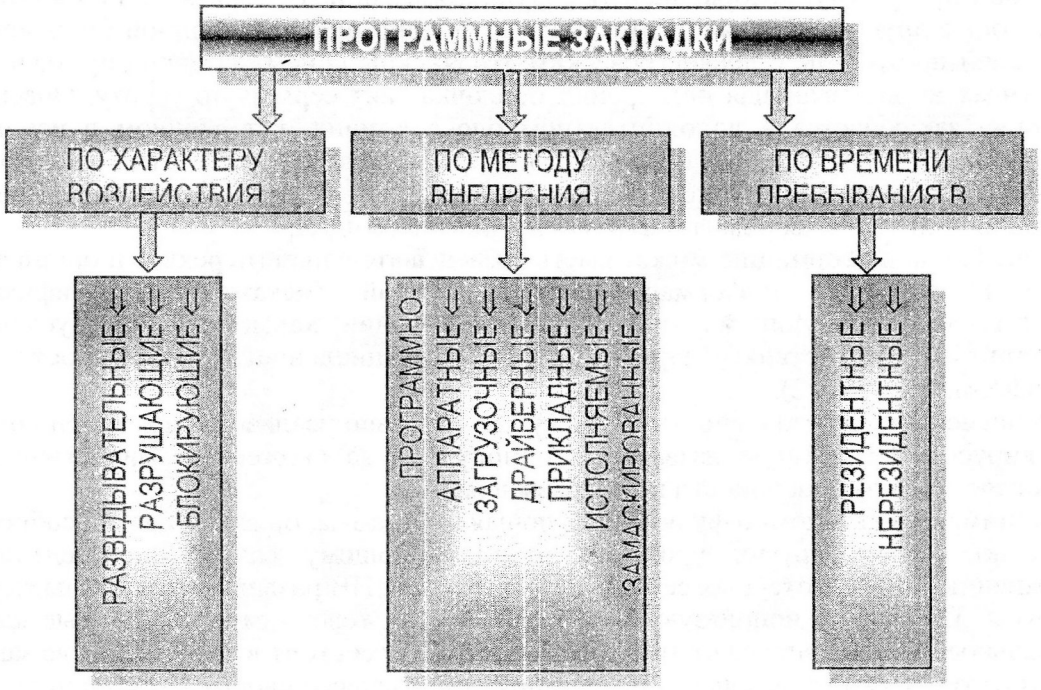




Рис. 2. Классификация ПЗ

Вирусы являются прямым потомком «логических бомб», т.к. в чистом виде в системе никогда не присутствуют, а являются «врезками» чужеродного кода в программу-носитель, в качестве которой может оказаться любая прикладная или системная программа. Первые вирусы, достаточно примитивные, появились в 1987 г., и с этого времени их количество растет по экспоненте, достигнув к 2000 году несколько десятков тысяч видов [6, 8]. Например, по данным за 2004 г. [15, 16] наибольшее количество заражений в мире вызвали сетевые черви (77,19%)- вредоносные программы, имеющие функции распространения по Интернет (электронная почта, Web-сервисы, сетевые пейджеры, IRC-каналы и др.). На втором месте оказались компьютерные вирусы (16,33%), в основном макровирусы. И на третьем – троянские программы (6,49%).

*Специальные средства* в составе ИО служат для реализации физической атаки (уничтожения) или электромагнитного подавления наиболее значимых ИС противника. Критическими звеньями системы управления в первую очередь будут информационные средства, подавление, разрушение или уничтожение которых приведет к немедленному снижению его возможностей по управлению боевыми системами, силами и средствами, а значит, и по нанесению массированных высокоточных ответных ракетных ударов. Эти радикальные средства, как правило, используются лишь при подготовке и в ходе военного конфликта в качестве обеспечивающего или самостоятельного вида боевых действий. Примерами применения подобного ИО являются военные действия США и их союзников во

имя войны с Ираком и воздушной кампании в Югославии. В обоих конфликтах американские силы предприняли большие усилия для разрушения и уничтожения «нервной системы» противника с целью ослабления способности сопротивляться или вести борьбу у противоборствующей стороны [10, 12].

Важной составляющей современных ИВ являются *информационно-психологическая обработка* населения и манипуляция общественным мнением. Некоторые специалисты в этой области называют ее еще «консциентальной» (с лат. conscientia – «сознание») составляющей войны.

Игнорирование этой составляющей сегодня, с учетом реалий мирового информационного простора, может приводить к плачевным результатам. Например, в [20] отмечалось, что в ходе 1-ой чеченской войны (1994-1996 гг.) проигранная исполнительными и военными органами России информационная война, как в теории, так и в практике, способствовала принятию неправильных, а порой и вредных решений по исключению чеченского синдрома. Отличительной чертой 2-ой чеченской войны является правильно поставленная федеральной властью идеологическая работа с российским обществом и СМИ. Как следствие, несмотря на значительные людские потери со стороны военнослужащих и мирного населения, на возникновение сложной гуманитарной ситуации и постоянного давления (порой предвзятого и субъективного по своей сути) со стороны Запада, это существенным образом не сказывается на общественном мнении россиян о проводимой антитеррористической операции.

Для реализации проекта информационно-психологической обработки не только противника, но и собственного населения, вскоре после событий 11 сентября 2001 г. в США создано Управление стратегического влияния (Office of Strategic Influence).

Сразу после его создания из стен этого ведомства начали рассылаться засекреченные предложения, в которых содержатся призывы использовать не только иностранные СМИ и Интернет, но и проводить тайные операции. Например, вбрасывать новостную информацию определенного толка в иностранные СМИ через персонал фирм, не замеченных в связях с Пентагоном [10-12]. Оружие информационно-психологического воздействия (голографические изображения в атмосфере, синтезаторы голосов известных политических лидеров, психотронное оружие, методы парапсихологии и биоэнергетики, «зомбирование» личности и т.д.) является важным видом ИО, которое постоянно опробуется и модернизируется США в ходе всех упоминавшихся выше локальных военных конфликтов. Сегодня комплексное использование различных способов скрытого психологического принуждения людей, разнообразных операций, пропагандистских акций и рекламных кампаний выступает как распространенное средство политической борьбы не только в международных, но и во внутриполитических конфликтах [1-3].

В целом, ИО характеризуется высокой скрытностью (возможностью действия без объявления войны), универсальностью применения, многовариантностью реализации и использования, большой разрушительной силой при относительно низкой стоимости. ИО может действовать избирательно, обходить трансграничные связи, что может сделать невозможным выявление источника атаки. Расходы США за последние 15 лет на разработку и приобретение средств ИО выросли в 4 раза и занимают ныне первое место среди всех военных программ [11].

Поэтому ИО сегодня рассматривается как идеальное средство для террористов, а информационный терроризм может стать угрозой существованию целых государств, что делает вопрос информационной безопасности важным аспектом национальной и международной политики [16].

Американские эксперты отмечают, что уже более 20 стран планируют и осуществляют различные виды информационных операций, направленных против Соединенных Штатов [10]. В отличие от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания. Германия включает управление средствами массовой информации как элемент информационной войны. Французы рассматривают концепцию информационной войны, состоящей из двух главных элементов: военной и экономической (или гражданской).

Французское представление принимает намного более широкое и более глубокое представление для конфликта в экономической сфере. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США. Французы даже имеют экономическую школу для информационной войны [10]. По мнению китайских военных аналитиков [14], последние войны и локальные конфликты показали, что «*информация и знание изменили предшествующую практику измерения военной силы простым подсчетом количества бронедивизий, авиакрыльев и авианосных групп. В настоящее время необходимо учитывать некоторые невидимые силы, как, например, возможности компьютеров, емкость коммуникаций и надежность информационной системы государства в целом*».

Таким образом, можно предположить, что будущие ИВ будут направлены не столько на физическое разрушение и уничтожение противника, сколько на разрушение или изменение его сознания. Превосходство над противником будет достигаться через преимущество в получении разнотипной информации, в мобильности, быстроте реакции, в точном огневом и информационном воздействии в реальном масштабе времени по многочисленным объектам его экономики, военным объектам и при минимально возможном риске для своих сил и средств. Однако в отличие от ударного высокоточного оружия, которое поражает конкретный, специально выбранный важный объект или его критическую точку, информационное оружие станет системоразрушающим, то есть выводящим из строя целые боевые, экономические или социальные системы.

Несомненно, что технологически развитые государства, в крайнем случае некоторые, будут стремиться увеличить политическое, экономическое и военное преимущество за счет установления и ведения глобального информационного контроля над менее развитыми государствами, проведения в мировом информационном пространстве идеологической и культурной экспансии [9].

***Вывод.*** Указанные обстоятельства требуют дальнейшего развития методологических и практических основ информационной безопасности как фундамента для обеспечения защиты национальных интересов Украины в информационной сфере и создания национальной системы информационной безопасности Украины. Степень защищенности государства, личности от рассмотренных видов ИО во многом определяет достигнутый (реальный) уровень их информационной безопасности.

**Список литературы**


1. Лисичкин В. А., Шелепин. Л. А. Третья мировая (информационно-психологическая) война. – М.: Институт социально-политических исследований АСН. – 1999. – 304 с.
2. Почепцов Г. Информационные войны. Основы военно-коммуникативных исследований. – К.: Ваклер, 2000. – 576 с.
3. Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны // Конфидент. – 1996. – №4. – С. 9-12.
4. Завадский И. И. Информационная война – что это такое? // Конфидент. – 1996. – №4. – С. 13-20.
5. Емельянов С. Л., Гаращук В. В. Практикум по основам информационной безопасности / О.: Юридическая литература, ОНЮА, 2005. – 112 с.
6. Емельянов С. Л. Основы информационной безопасности / Конспект лекций. – О.: Юридическая литература, ОНЮА, 2003. – 198 с.
7. Емельянов С. Л. Некоторые аспекты информационной безопасности как интегральной проблемы // Наук. записки Міжнар. гуманіт ун-ту. Випуск 1. – Одеса: МГУ, 2004. – С. 165-170.
8. Емельянов С. Л., Яковлев И. А. Принципы построения комплексной системы антивирусной защиты // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Наук. -техн. збірник. Випуск 8. – Київ, 2004. – С. 124-129.

9. Горбенко І. Д., Долгов В. І., Гріненко Т. О. Інформаційна війна -- сутність, методи та засоби ведення // Матер. ювілейної наук. -техн. конф. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Київ, 1998. – С. 11–15.
10. Гриняев С. Н. Информационная война: история, день сегодняшний и перспективы (http://www. agentura. ru).
11. Леваков А. Новые приоритеты в информационной безопасности США (http://www. agentura. ru).
12. Слипченко С. Информационное противоборство в бесконтактных войнах (http://kiev-security. org. ua).
13. Гриняев С. Н. Особенности информационной войны во время агрессии НАТО против Югославии (http://www. agentura. ru).
14. Ешихара Т. Китайская информационная война (http://abirus. ru).
15. http://www. crime-research. org. ua: Центр исследования проблем компьютерной преступности.
16. Интервью бывшего директора ФАПСИ А. Старовойтова (http://www. agentura. ru).
17. Красноступ Н., Кудин Д.. Шпионские программы и новейшие методы защиты от них // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Наук. -техн. збірник. Випуск 9. – Київ, 2004. – С. 67–75.
18. Барсуков В. С., Дворянкин С. В., Шеремет И. А. Методы и средства обеспечения безопасности в информационно-вычислительных сетях общего пользования// Технологии электронных коммуникаций. – Т. 20. – М.: 1992. – С. 65-96.
19. Климов В. Промышленный шпионаж как основа информационных войн (http://www. fakt. ru).

*Поступила 3.03.2008г.*

УДК 004.683

С.А. Печень

## АНАЛИЗ РАБОТЫ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕВЫХ РЕСУРСОВ

Наиболее распространенные средства защиты, согласно ежегодным отчетам CSI/FBI Security Survey, данные за 2007 год представлены в таблице 1[1]:

Таблица 1

**Наиболее часто используемые технологии безопасности[2,3]**

| Место | Используемая технология | Процент использования данной технологии |
|---|---|---|
| 1 | Антивирусное ПО | 98 |
| 2 | Межсетевые экраны | 97 |
| 3 | Виртуальные частные сети | 84 |
| 4 | Антишпионское ПО | 80 |
| 5 | Системы обнаружения вторжений | 69 |
| 6 | Шифрование передаваемых данных | 66 |
| 7 | Управление обновлениями | 63 |
| 8 | Списки управления доступом | 56 |