УДК 623.618:519.686

ИНФОРМАЦИОННОЕ ОРУЖИЕ ЗАЩИТЫ КАК НОВЫЙ КЛАСС ВООРУЖЕНИЯ ПРИ ПРОВЕДЕНИИ ИНФОРМАЦИОННЫХ ОБОРОНИТЕЛЬНЫХ ОПЕРАЦИЙ

С.А. Сидченко, к.т.н. К.И. Хударковский, к.т.н. В.Л. Петров
(представил д.т.н., проф. А.А. Рось)

По материалам открытой отечественной и зарубежной печати, средств массовой информации и онлайновых источников впервые проведена систематизация и анализ разрозненных сведений о видах и средствах информационного оружия защиты как нового класса вооружения при проведении информационных оборонительных операций

Постановка проблемы. Настоящий момент времени характеризуется активными исследованиями сущности информационной борьбы и современных проблем информационной безопасности государства как фактора противодействия информационным войнам [1 – 5]. Это привело к резкому увеличению роли информационного оружия (ИО) как наступательного, так и оборонительного характера.

Результаты анализа подготовки и проведения последних военных и вооруженных конфликтов в Югославии, Афганистане, Чечне и Ираке показывают высокую эффективность методов информационной войны [1].

Поэтому приоритетными направлениями в обеспечении информационной безопасности государства являются “створення засобів захисту від несанкціонованого доступу до інформаційних ресурсів та від порушення нормального функціонування комп’ютерно-телекомунікаційних мереж”, “нейтралізація інформаційно-психологічних впливів проти держави” [1] и др. Все это требует разработки новых видов информационного оружия для защиты информационного пространства государства. Для этого необходимо систематизировать и провести анализ разрозненных сведений об уже имеющемся и перспективном информационном оружии для защиты автоматизированных систем управления (АСУ) войсками и оружием и информации, циркулирующей в них.

Анализ литературы. Рассмотрению вопросов определения, классификации и особенностей информационного оружия посвящены работы [2 – 9]. Так в [2] дана классификационная основа информационного оружия, а в [9] проведены систематизация и анализ видов информацион-

ного оружия, применяемого при проведении информационных наступательных операций.

В [9] сделан вывод о том, что понятие “информационное оружие” содержит в себе высокую степень абстрактности обобщения, что открывает для дальнейших исследований пути универсального отражения сущности традиционных и новых классов вооружения и военной техники в новых условиях противоборства в информационном (в широком смысле) пространстве с единых философских позиций.

Однако во всех этих источниках информационное оружие рассматривается только с точки зрения дезорганизации АСУ противника.

Цель статьи. По материалам открытой отечественной и зарубежной печати, средств массовой информации и онлайновых источников систематизировать и проанализировать разрозненные сведения о видах и средствах информационного оружия для защиты информационного пространства государства в ходе информационной оборонительной операции. Конкретизировать сущность, основные виды и свойства информационного оружия, комплексы и средства, обеспечивающие его применение и объекты воздействия при защите автоматизированных систем управления войсками и оружием.

Изложение основного материала. Под **информационной операцией** понимается совокупность согласованных по цели, задачам, месту и времени информационных воздействий, атак и битв, проводимых по единому замыслу и плану для решения задач информационной борьбы на стратегическом или оперативном направлении [3]. При этом **информационные оборонительные операции** включают проведение различных мероприятий с использованием средств и методов противодействия эффективному применению информационного оружия противника [2]. Особенность информационной борьбы (войны) заключается в необходимости одновременного проведения наступательных и оборонительных операций.

Под **информационным оружием** защиты будем понимать совокупность специальных информационных, программно-аппаратных, технических, радиоэлектронных, психологических и организационных систем, средств и мероприятий, применяемых для противодействия деструктивным воздействиям на автоматизированные системы управления и информационные ресурсы своей группировки войск, а также сознание (и подсознание) личного состава (рис. 1).

1. Информационное оружие защиты программно-математического обеспечения АСУ и информационных ресурсов. Под ним будем понимать совокупность программно-аппаратных методов и средств,

а также организационных мероприятий по защите элементов АСУ, программного обеспечения и информационных ресурсов.

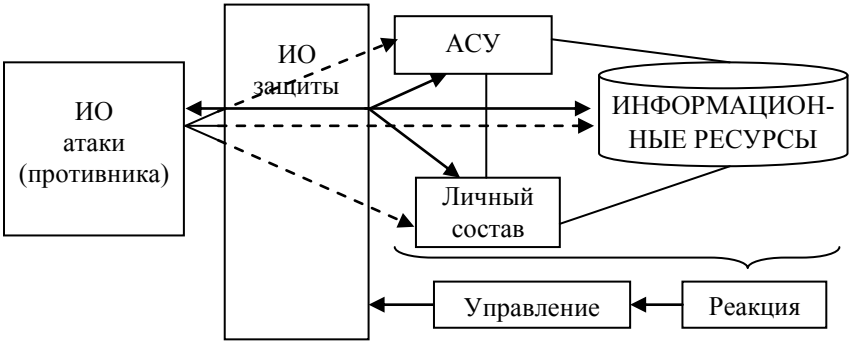

Рис. 1. Схема взаимосвязи информационного оружия наступательного и оборонительного характера

Основными средствами защиты являются:

– средства мониторинга состояния АСУ (например, программа-трассировщик VisualRoute, наглядно показывающая пользователю все передвижения по сети Интернет);

– средства защиты операционных систем;

– средства идентификации и контроля доступа;

– антивирусы (AVP или антивирус Касперского, UNA или Украинский национальный антивирус, DrWeber, AidsTest, Norton AntiVirus, McAfee VirusScan и др.);

– вирусы защиты (гипотетически возможны, например, Macro-вирусы для защиты документов);

– брандмауэры (межсетевые экраны) и антиспамы (например, Norton Internet Security, Kaspersky Anti-Hacker, Kerio Personal Firewall, ZoneAlarm, FireWall-1 фирмы CheckPoint, Antiy Ghostbusters фирмы Antiy Lab и др.);

– криптографические средства защиты (шифрования, хеширования, цифровой подписи, стеганографические преобразования, скремблеры и т.д.);

– средства семантической и фонетической «маскировки»;

– средства контроля целостности и достоверности информации (например, программа-антивирус контроля модификации файлов McAfee VirusScan);

– средства восстановления после сбоя (например, программа восстановления файлов BadCopy);

– другие.

2. Информационное оружие нейтрализации информационно-психологических воздействий. В его составе могут применяться:

– **средства воздействия на сознание и подсознание личного состава (психотронные средства).** К данной группе могут относиться средства массовой информации (радио, пресса, телевидение) и агитационно-пропагандистские средства (видеокассеты, электронные учебники и энциклопедии и др.), предназначенные для целенаправленного информационно-психологического (пропагандистского) воздействия на свой личный состав с целью формирования духовных ценностей и морально-нравственных идеалов, противодействия дезинформации, психологической;

– реабилитации личного состава и управления кризисом. К данной группе относится и предложенное авторами специальное программное обеспечение «WordSD», предназначенное для оценки воздействия слов и текстов (выступлений) на подсознание человека и формирование текстов с заданными характеристиками целенаправленного воздействия;

– **средства воздействия на нейро-мозговой субстракт личного состава (психотропные средства)** – специальные лекарственные препараты-антидепрессанты, предназначенные для воздействия на психику личного состава на генном или хромосомном уровнях с целью психологической реабилитации личного состава;

– **средства «социальной инженерии»** – одной из частей социальной психологии, направленной на манипулирование людьми или порождение в их разуме новой модели поведения.

3. Информационное оружие противодействия физическому уничтожению элементов АСУ. К данному виду ИО отнесем системы и средства, противодействующие физическому разрушению элементов АСУ: системы и средства огневого поражения информационного наступательного оружия противника (наземные системы и средства, самолеты, вертолеты и беспилотные летательные аппараты огневого поражения, разведки, радиоэлектронного подавления, АСУ и КП, системы высокоточного оружия) и маскировки элементов своих АСУ.

4. Информационное оружие радиоэлектронной защиты (противодействия). Под информационным оружием радиоэлектронного противодействия будем понимать, с одной стороны, комплексы и средства радиоэлектронного подавления (РЭП) ИО противника, а с другой – комплекс организационных и технических мероприятий по обеспечению эффективного и устойчивого функционирования АСУ в условиях ведения противником РЭП, разведки и взаимного влияния радиоэлектронных систем при их совместной работе. В Вооруженных Силах Украины задачи по радиоэлектронному подавлению ИО противника могут решать:

– для радиоэлектронного подавления многофункциональных бортовых радиолокационных станций станции СПН-30, СПН-40, СПО-8 (дальность действия 15 – 150 км);

– для подавления высокоточного оружия, например, радиоуправляемых снарядов – станция Р-934Б (дальность действия больше 100 км).

Радиоэлектронная защита своих АСУ реализуется с помощью технических мер, основанных на использовании селективных свойств радиоприемных устройств и использовании сложных избыточных структур сигналов и соответствующих алгоритмов обработки, а так же радиоэлектронным оборудованием позиционных районов.

5. Информационное оружие разведки и контрразведки. К данному виду относится вся совокупность систем, средств и мероприятий разведки и контрразведки, включая их проведение и в кибернетическом пространстве.

Под «киберразведкой» будем понимать комплекс мероприятий по добыванию, обработке и анализу разведывательной информации в кибернетическом (телекоммуникационном) пространстве, а под «киберконтрразведкой» – комплекс мероприятий по противодействию «киберразведке» (в качестве средств «киберразведки» могут применяться «поисковые машины», а «киберконтрразведки» – антиспамы).

Кроме этого, к этому виду можно отнести и системы моделирования боевых действий (алгоритмы и модели), позволяющие принять оптимальное (квазиоптимальное) решение без потерь личного состава.

Рефлексивное управление защитой. Управление защитой проводится с целью контроля целостности систем и средств ИО и повышения эффективности мероприятий по противодействию деструктивным действиям противоборствующей стороны. Рефлексивное управление позволяет создать динамическую защиту, основанную на многократном отображении в памяти системы, принимающей решение, представлений о возможностях и целевых функций противоборствующей стороны. Основные подходы к рефлексивному управлению рассмотрены в [2].

Свойства информационного оружия защиты как нового класса вооружения и военной техники. Основными свойствами информационного оружия являются:

– наличие «информационного боеприпаса» и/или «информационного элемента противодействия»;

– наличие средств управления и «элемента наведения на информационный боеприпас»;

– наличие средств доставки и высокая их скорость;

– скрытность организации воздействия и противодействия;

– широкий диапазон дальностей воздействия;
– комплексность воздействия;
– рассредоточенность.

Анализ свойств указывает на то, что понятие “информационное оружие защиты” является многогранным по характеру своего проявления, особенно на концептуальном уровне, когда речь идет о сущности механизмов планирования и ведения информационных операций.

Объектами воздействия ИО защиты являются информационные ресурсы, АСУ, личный состав собственной группировки и ИО и информационные ресурсы противоборствующей стороны. В качестве субъектов защиты могут выступать специальные подразделения информационной борьбы, информационные комплексы и оружие. В качестве противоборствующей системы может выступать глобальная система информационного контроля «Эшелон», созданная Агентством национальной безопасности США, и аналогичная гипотетически существующая система СОУД – «Система оперативных и учрежденческих данных», принадлежащая ГРУ и КГБ России.

Классификация, предложенная в [2], может быть расширена за счет **классификации для ИО защиты**:

1) по характеру противодействия:
   - пассивное оружие;
   - активное оружие;
2) по способу воздействия на информацию, информационные процессы и ИО нападения:
   - оружие противодействия;
   - оружие превентивного действия;
   - оружие управления (контроля целостности);
3) по наличию обратной связи с объектом воздействия:
   - с обратной связью;
   - без обратной связи;
4) по расположению объекта воздействия:
   - внутрисегментное;
   - межсегментное.

Выводы. В статье впервые рассмотрен подход к информационному оружию с точки зрения его защитных функций.

Многообразие объектов ИО, разрозненный характер разработок в области его создания и применения делают необходимым введение универсальных показателей боевой эффективности и критериев сравнения различных видов ИО и существующих видов вооружения и военной техники для выбора их видов и объектов воздействия.

Показатели эффективности применения информационного оружия должны комплексно учитывать боевой потенциал вида ИО и экономические аспекты его разработки (либо закупки), применения по назначению, технической эксплуатации и ремонта. Это позволит обоснованно принимать решение на разработку, дополнительное производство, модернизацию и закупку современных видов ИО, которые будут соответствовать мировым стандартам.

ЛИТЕРАТУРА

1. *Толубко В.Б., Жук С.Я., Косевцов В.О. Концептуальні основи інформаційної безпеки України // Наука і оборона. – 2004. – № 2. – С. 19 – 25.*
2. *Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія. – К.: НАОУ, 2003. – 320 с.*
3. *Руснак І.С., Телелим В.М. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі // Наука і оборона. – 2000. – № 2. – С. 18 – 23.*
4. *Попов М.О., Лук'янець А.Г. До забезпечення воєнної безпеки в умовах загрози інформаційної війни // Наука і оборона. – 1999. – № 2. – С. 37 – 43.*
5. *Толубко В.Б., Рось А.О. Складові інформаційної боротьби // Наука і оборона – 2002. – № 2. – С. 23 – 28.*
6. *Гриняев С.Н. Интеллектуальное противодействие информационному оружию. (Серия «Информатизация России на пороге XXI века».) – М.: СИНТЕГ, 1999. – 232 с.*
7. *Маначинский А. Третья мировая война: информационная война // Человек и закон. – 2000. – № 3 (4). – С. 32 – 37.*
8. *Шаравов И. К вопросу об информационной войне и информационном оружии // Зарубежное военное обозрение. – 2000. – № 10. – С. 2 – 5.*
9. *Шолохов С.Н., Сидченко С.А. Информационное оружие – новый класс вооружения для дезорганизации АСУ войсками и оружием при проведении информационных наступательных операций // Сборник научных трудов ХВУ. – Х.: ХВУ. – № 1 (39). – 2002. – С. 10 – 14.*

Поступила 5.11.2004

СИДЧЕНКО Сергей Александрович, *старший научный сотрудник НИО НПВО ХУПС. В 1994 году окончил ХВУ. Область научных интересов – информационная борьба и криптографические системы защиты информации.*

ХУДАРКОВСКИЙ Константин Игоревич, *кандидат технических наук, доцент, старший научный сотрудник НИО НПВО ХУПС. В 1989 году окончил Харьковское ВВКИУ РВ. Область научных интересов – информационная борьба и техническая защита информации.*

ПЕТРОВ Вадим Лукьянович, *канд. техн. наук, доцент, старший научный сотрудник ОНИИ ВС. В 1978 году окончил ВИРТА ПВО. Область научных интересов – информационная борьба.*