УЧРЕДИТЕЛИ:
РЕГИОНАЛЬНОЕ СОДРУЖЕСТВО В ОБЛАСТИ СВЯЗИ,
МЕЖДУНАРОДНАЯ АКАДЕМИЯ СВЯЗИ,
РОССИЙСКОЕ НАУЧНО-ТЕХНИЧЕСКОЕ ОБЩЕСТВО
РАДИОТЕХНИКИ, ЭЛЕКТРОНИКИ И СВЯЗИ
ИМ. А.С. ПОПОВА

ЭЛЕКТРОСВЯЗЬ
ОСНОВАН В 1933 ГОДУ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ
ПО ПРОВОДНОЙ И РАДИОСВЯЗИ,
ТЕЛЕВИДЕНИЮ, РАДИОВЕЩАНИЮ

№ 8/2008

Индексы 71107. ISSN 0013-5771.
ЭЛЕКТРОСВЯЗЬ. 2008, № 8. 1-64.
Сдано в набор 10.08.2008.
Подписано в печать 23.08.2008.
Печать офсетная. Формат 60×90 1/8.
Изд. № 62. Усл. кр.-отт. 14,12.
Уч.-изд. л. 19,6. Усл. печ. л. 8.
Тираж 3000 экз.

В НОМЕРЕ:

CONTENTS

Адрес редакции журнала: 107031, Москва, К-31, Кузнецкий мост, д. 20/6.
Тел.: 625-84-36, 621-09-13, 624-15-92. Факс: 624-52-90.
E-mail: elsv@garnet.ru Internet: www.elsv.ru

ISSN 0013-5771. «ЭЛЕКТРОСВЯЗЬ», № 8, 2008

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

С возникновением в конце XX — начале XXI века Глобального информационного общества, наряду с громадными возможностями, которые в связи с этим открылись перед человечеством, появились серьезные проблемы, не известные ранее, а именно — преступное использование инфокоммуникационных сетей и систем, а также противоправное воздействие на них.

Информационная среда — системообразующий фактор жизни любого общества. Она активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности. Национальная безопасность любого государства и мирового сообщества в целом существенно зависит от уровня информационной безопасности, и в ходе технического прогресса эта зависимость, несомненно, будет возрастать.

Предлагаем вниманию читателей беседу нашего корреспондента с заместителем руководителя Службы контрразведки — начальником Центра информационной безопасности Федеральной службы безопасности Российской Федерации (ФСБ России) генерал-лейтенантом В.В. Скориком.

***Биографическая справка.* Родился в 1951 г. Окончил Куйбышевский авиационный институт им. С.П. Королева, затем — Высшую школу КГБ СССР. В органах безопасности с 1977 г. Лауреат Премии правительства РФ в области науки и техники, имеет звание «Заслуженный сотрудник органов безопасности Российской Федерации», другие государственные и ведомственные награды.**

Владимир Владленович, очевидно, что борьба с преступностью в информационной среде, иными словами, кибертерроризмом, является составной частью обеспечения и национальной, и международной информационной безопасности (МИБ). Расскажите, пожалуйста, какова ситуация с МИБ сегодня и как участвуют в решении этой проблемы специалисты ФСБ?

Начну с того, что проблемам МИБ большое внимание уделяет Организация Объединенных Наций. Кроме того, вопросы противодействия кибертерроризму активно обсуждаются в формате Шанхайской организации сотрудничества (ШОС). По решению глав государств ШОС образована группа экспертов по вопросам международной информационной безопасности, которая подготовила два документа: План действий и Решение Совета глав государств-членов ШОС.

Документы предусматривают проведение совместных мероприятий в сфере обеспечения МИБ, включая противодействие использованию IT-технологий в террористических целях, борьбу с компьютерной преступностью, мониторинг сети Интернет и т. д.

Вопросы МИБ регулярно обсуждаются также в рамках мероприятий «Группы восьми». В период председательства Российской Федерации в «Восьмерке» проблема кибертерроризма была включена в повестку дня Римско-Лионской группы экспертов. Разработаны основы стратегии стран «Восьмерки» в области информационной безопасности. Кроме того, возникла тенденция к организации региональных форумов, которые будут рассматривать вопросы МИБ применительно к местным условиям. В частности, такие предложения высказывали представители ряда латиноамериканских и африканских стран.

Из приведенных примеров видно, что проблемы МИБ вызывают озабоченность многих международных организаций и всего мирового сообщества.

Эксперты ФСБ регулярно принимают участие в конференциях и рабочих встречах, касающихся проблем киберпреступности, проводимых как на двухстороннем, так и многостороннем уровнях. Каждый раз мы стремимся вносить конструктивные предложения при рассмотрении, несомненно, сложных вопросов международной информационной безопасности. Ведь преступный мир мгновенно реагирует на изменение ситуации, поэтому прогресс в области информатики не остался без внимания криминалитета и его наиболее опасной части — террористов и экстремистов. Они незамедлительно взяли на вооружение телекоммуникационный инструментарий.

Каковы наиболее часто встречающиеся виды киберпреступлений?

Исходя из их источников, преступления или, как говорят профессионалы, вызовы и угрозы международной информационной безопасности, можно условно разделить на три группы.

Первая. Это преступления в сфере информатики, совершаемые криминальными элементами и структурами. К ним относятся: неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, нарушение нормальных условий эксплуатации компьютерных сетей. Киберпреступность проявляется в разнообразных формах, включая виртуальные финансовые операции, хищение паролей и кодов доступа, персональных и корпоративных коммерческих сведений, взлом сайтов, рассылку спама, противозаконное распространеие информации — список можно продолжить.

Причем мошенники не ограничиваются рамками Интернета — они совершают преступления, где информационные ресурсы и вычислительная техника выступают объектами криминальных посягательств либо средой или орудием преступления.

Вызовы и угрозы МИБ *второй* группы исходят от экстремистов, террористов и их организаций. Существо этих угроз заключается в использовании IT-технологий:

- для совершения диверсионно-террористических операций с использованием компьютерных сетей, что подразумевает вмешательство в сети или их разрушение в целях воздействия на процесс принятия решений органами государственной власти и международными организациями, а также нападение на компьютерные системы, обеспечивающие управление военными, промышленными, энергетическими, транспортными объектами, финансовыми структурами;
- распространения идеологии терроризма и экстремизма, подстрекательства к террористической деятельности;
- создания преступных сообществ с целью вербовки, вооружения, обучения террористов и совершения терактов;
- оперативного руководства террористическими акциями;
- финансирования террористической деятельности;
- распространения дезинформации и угроз с паническим вектором с целью психологического воздействия на население.

О размахе этой деятельности можно судить по тому, что на сегодняшний день общее количество сайтов террористической направленности в Сети превысило 4000.

Третья группа вызовов и угроз МИБ кроется в соблазне применения IT-технологий в межгосударственных отношениях для обеспечения военно-политического превосходства и оказания силового давления.

Доминирование отдельных стран в области информатики, углубление «цифрового разрыва» между государствами могут повлечь за собой региональное и глобальное изменение баланса сил, появление в мире новых центров конфронтации. Все чаще в средствах массовой информации, в научных трудах, на профильных конференциях употребляется термин «информационное оружие». В первом приближении под ним можно понимать средства и методы нанесения ущерба информационным ресурсам государств, негативного воздействия на их критические инфраструктуры, а также дестабилизирующей психологической обработки населения. Не вдаваясь в юридические нюансы этого определения, хочу, тем не менее, подчеркнуть, что объективная реальность практического применения информационного оружия вряд ли может вызвать у кого-либо сомнения и не должна быть проигнорирована.

Среди характерных черт информационного оружия следует отметить его универсальность, трансграничность, относительную дешевизну и доступность. В силу ряда причин информационное оружие представляет собой особую опасность.

Во-первых, его применение легко закамуфлировать под другие виды деструктивных информационных воздействий, а реальный источник и государственная принадлежность этого оружия будут надежно скрыты в киберпространстве. В конечном счете агрессия может осуществляться латентно с территории третьих стран, которые даже не будут подозревать об этом.

Во-вторых, наращивание военно-информационного потенциала может преподноситься как неизбежное следствие научно-технического прогресса.

В-третьих, в ходе милитаризации информационного пространства широко используются средства двойного назначения, что позволяет создавать информационное оружие скрытно, в рамках научно-исследовательских программ общего назначения.

В-четвертых, кажущаяся гуманность информационного оружия, которое не направлено напрямую на людей, может облегчить принятие политического решения об информационной атаке, в то время как ее воздействие на критические инфраструктуры будет иметь катастрофический характер, сопоставимый с применением оружия массового уничтожения.

В-пятых, некоторые разновидности информационного оружия в силу простоты их создания и применения могут быть использованы не только военными структурами, но и террористическими организациями.

Владимир Владленович, а есть ли данные, какие страны ведут разработки информационного оружия?

Могу только сказать, что, согласно экспертным оценкам, сегодня около 120 стран находятся на разных этапах создания средств деструктивного информационного воздействия. Для сравнения: разработку ядерных вооружений ведут не более 20 государств.

Еще раз хочу подчеркнуть, что проблема международной информационной безопасности относится к разряду актуальнейших, и ее полномасштабное решение возможно только при комплексном рассмотрении триады угроз: преступного, террористического и военно-политического характера.

Единство проблематики МИБ должно базироваться на том, что и хакеры, и виртуальные террористы, и военные действуют в едином информационном пространстве, используют методы и средства, которые близки по своему назначению и техническим принципам, нацелены на одни и те же объекты.

В силу неделимости глобального киберпространства, а также масштабности вызовов и угроз мировой стабильности проблему МИБ не удастся решить ни на региональ-