**Глобальная информация и безопасность**

Содержание

Введение 2

1. Факторы угрозы безопасности информационного пространства 3

2. Государственно-правовое обеспечение безопасности информационного пространства 6

3. Методы обеспечения безопасности информационного пространства 8

Заключение 12

Литература 13

## Введение

В современном информационном обществе информация превратилась в особый ресурс любой деятельности, следовательно, как и всякий другой ресурс, нуждается в защите, в обеспечении ее сохранности, целостности и безопасности.

Информационное пространство России в настоящее время бурно развивается, создаются информационно-телекоммуникационные структуры, развиваются сети мобильной связи, телевидение и другие составляющие информационной инфраструктуры, обеспечивающие обмен как внутри страны, так и с зарубежными источниками информации. Все больше и больше становится пользователей сети Интернет. Появились официальные интернет-представительства органов государственной власти Российской Федерации. Все это позволяет постоянно расширять возможности граждан по реализации их прав на получение и распространение информации, что является гарантией развития личности и общества, совершенствования государственного механизма.

С другой стороны, интенсивное внедрение информационных технологий в сферы деятельности личности, общества и государства, а также с широкое применение открытых информационно-телекоммуникационных систем, интеграция отечественных информационных систем и международных информационных систем повышает вероятность применения «информационного оружия» против информационной инфраструктуры России.

## 1. Факторы угрозы безопасности информационного пространства

Угрозы в информационном пространстве обусловлены как объективными, так и субъективными факторами. К *объективным* факторам следует отнести последствия стихийных бедствий, экологических или техногенных катастроф. К *субъективным* факторам относятся преднамеренные или непреднамеренные действия участников информационного обмена, приводящие к возникновению чрезвычайных ситуаций, а также ошибки и недостатки при проектировании, создании и эксплуатации информационно-телекоммуникационных систем, обусловленные недостатком квалификации разработчиков или отсутствием необходимых финансовых средств у заказчиков информационно-телекоммуникационных систем. Следует признать, что существенной особенностью стратегических рисков в информационном пространстве является доминирование субъективного фактора возникновения чрезвычайных ситуаций над объективным фактором. Роль субъективного фактора еще более возросла с появлением компьютерного терроризма (или кибертерроризма).

Среди источников возникновения чрезвычайных ситуаций в информационном пространстве, являющихся проявлением субъективного фактора, особо следует выделить компьютерные вирусы, в том числе троянские программы, сетевые черви, логические бомбы. Так, по оценкам экспертов, 2 из 3 электронных послания содержат «спам», каждое 208 послание содержит вирус, каждый день в среднем обнаруживается около 20 новых вирусов. Россия находится на одном из ведущих мест по количеству создания новых вирусов, а основную угрозу для информационной системы предприятий представляют собственные сотрудники.

Как отмечалось в докладах участников 2-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» (18 июня 2001 г., Москва), даже согласно официальным данным, состояние информационной безопасности не просто оказывается тревожным, но продолжает быстро ухудшаться. По статистике российского представительства SARC (Symantec Antivirus Research Center) для нашей страны характерны следующие тенденции:

1. Количество файлов-вирусов, отсылаемых на экспертизу в этот центр, медленно, но уверенно растет;

2. Процент содержания новых вирусов в файлах, отправленных из России, является одним из самых высоких в мире (примерно в 10 раз выше, чем в целом по Европе);

3. Уровень защищенности и информатизации в нашей стране один из самых низких в мире.

По данным Международного Института Компьютерной Безопасности (ICSA), среднестатистическая вирусная атака на сервер обходится компании в 8366 долларов. В результате заражения происходит примерно 40-минутный простой машины, после чего еще 44 минуты требуется на восстановление сервера. Простой людских ресурсов за это время составляет 22 человекодня. 22% фирм, занимающихся продажами через Интернет, фиксировали потери информации, а 12% столкнулись с кражей данных и торговых секретов. Согласно данным ФБР, вирусы являются причиной финансовых потерь в 76% случаев. Далее следуют ошибки из-за невнимательности персонала, атаки изнутри и извне.

Кризисные ситуации в информационном пространстве России, как правило, являются последствиями разного рода воздействий на информационно-телекоммуникационные системы, в результате которых становится невозможным доступ к информационным ресурсам, искажается информация, нарушаются права собственности на информацию или правила ознакомления с информацией, содержащей сведения, составляющие государственную тайну, или сведения ограниченного доступа. Однако не всякое нарушение приводит к чрезвычайной ситуации, когда причинен ощутимый ущерб участникам информационного процесса, экономически важным системам, интересам государства. Например, заражение компьютерным вирусом одного домашнего персонального компьютера, на котором не содержится уникальная информация, не приводит к чрезвычайной ситуации. С другой стороны, широкомасштабная вирусная атака, проводимая сетевым компьютерным DOS-вирусом, в результате которой выходят из строя целые сегменты компьютерной сети, приводит к чрезвычайной ситуации в информационном пространстве.

Угрозы безопасности информационного пространства побуждают к разработке комплекса мероприятий, направленных на снижение риска возникновения чрезвычайной ситуации. Для этого необходимо прежде всего определить совокупность угроз применительно к конкретному сегменту информационного пространства и допустимый уровень риска их реализации и оценить затраты на локализацию и ликвидацию последствий.

Наиболее сложной задачей является оценка величины вероятности реализации той или иной угрозы, а также тенденций изменения угроз при тех или иных условиях и появление новых угроз, обусловленных развитием информационных технологий. Так, развитие глобальной сети Интернет сделало реальностью угрозу вычислительного терроризма, заключающуюся в негласном использовании громадных вычислительных ресурсов сети Интернет для взлома информационных систем.

Мероприятия по предотвращению чрезвычайных ситуаций в информационном пространстве должны быть направлены на снижение существующих рисков реализации тех или иных угроз. Основой для проведения этих мероприятий является всесторонний анализ угроз применительно к конкретному сегменту информационного пространства. Важной составляющей этого анализа является определение механизмов и достаточных средств защиты для снижения рисков до приемлемого уровня. При этом должен соблюдаться принцип «разумной достаточности», чтобы использование средств защиты информационно-телекоммуникационных систем не снижало оперативность обработки и передачи информации. Следует также отметить, что эффективное предупреждение чрезвычайных ситуаций в информационном пространстве России возможно только на основе комплексного, системного подхода к решению этой проблемы.

## 2. Государственно-правовое обеспечение безопасности информационного пространства

Важнейшим механизмом повышения безопасности информационного пространства является государственно-правовое регулирование деятельности субъектов информационного обмена и рынка информационных услуг. Отправной точкой является законодательное обеспечение прав участников информационного обмена и определение степени их ответственности за возникновение чрезвычайных ситуаций. Примерами подобных законодательных актов являются Закон Российской Федерации «Об информации, информатизации и защите информации». Федеральный Закон «Об участии в международном информационном обмене», а также ряд Указов Президента Российской Федерации.

В июне 2000 г. президент России Владимир Путин утвердил доктрину информационной безопасности страны. Доктрина была одобрена на заседании Совета безопасности 23 июня 2000 г.

Первые попытки разработки доктрины в 1994 г. не увенчались успехом, и лишь в январе 2000 г. информационная сфера была включена в Концепцию национальной безопасности как самостоятельный фактор национальных интересов России. «Интенсивное развитие информационных технологий и интегрирование России в мировое информационное пространство, – подчеркнул первый заместитель секретаря Совета безопасности России Владислав Шерстюк. Шерстюк, поясняя необходимость принятия этой Доктрины, – сделали общество и государство в целом зависимыми от информационной среды, чего раньше не было».

40-страничный проект хорошо проработан и состоит из четырех разделов. В первом из них приведены виды и источники угроз информационной безопасности России и сформулированы задачи по ее обеспечению. Во втором изложены общие методы противодействия угрозам информационной безопасности и конкретика для различных сфер. В третьем раскрываются основные положения государственной политики обеспечения информационной безопасности и указываются мероприятия по ее реализации, а четвертый раздел касается организационной основы обеспечения информационной безопасности.

«Серьезную опасность, – подчеркивается в Концепции, – представляют собой стремления ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним».

В связи с этим, по мнению разработчиков доктрины, России прежде всего необходимо развивать индустрию средств информатизации, которая существенно отстает от мирового уровня. Их необходимость наглядно подтверждается данными МВД о наносимом России ущербе от компьютерной преступности.

Регулярно проводятся конференции, посвященные вопросам глобальной информации и безопасности. 5 февраля 2000 г. в Москве в рамках 6-го Международного форума «Технологии безопасности» прошла 1-я Всероссийская Конференция «Информационная безопасность России в условиях глобального информационного общества». Основные проблемы, которые обсуждались на конференции:

1. Принципы построения системы информационной безопасности России в условиях глобального информационного общества и направления развития правовой базы информационной безопасности в целях обеспечения интересов личности, общества и государства.
2. Задачи модернизации системы государственного управления, совершенствование государственного регулирования в области телекоммуникаций и информационных технологий, создание институтов общественного контроля.
3. Направления развития информационной и телекоммуникационной инфраструктур и технологий, задачи активизации производства, развития рынка, поддержки научно-технического потенциала.
4. Новый взгляд на системы управления в бизнесе и промышленности в условиях глобализации и информатизации общества. Сетевая экономика и Интернет-технологии.
5. Подготовка кадров, образование, формирование национальных информационных ресурсов.
6. Совершенствование государственной системы защиты прав интеллектуальной собственности (концептуальные, организационные и правовые аспекты).
7. Проблемы и перспективы модернизации институтов государственной, коммерческой и банковской тайны в условиях глобального информационного общества.
8. Проблемы защиты интересов личности, общества и государства в связи с развитием преступности в сфере высоких технологий.

7-я Всероссийская конференция «Информационная безопасность России в условиях глобального информационного общества» пройдет 26-27 января 2005 года в Москве.

## 3. Методы обеспечения безопасности информационного пространства

Говоря о средствах защиты информации, необходимо отметить, что сегменты рынка, нуждающихся в защите глобальной информации, достаточно разнообразны. В отдельные рынки выделяются системы, обеспечивающие государственную тайну, системы защиты в корпоративном секторе, интеграция различных продуктов в рамках одной системы. По словам специалистов, каждый проект имеет собственную специфику, и создание универсальных решений для различных отраслей является невозможным.

В настоящее время разработаны и продолжают совершенствоваться технологические основы защиты информационного взаимодействия в компьютерных сетях при их подключении к открытым коммуникациям, методы и средства межсетевого экранирования для защиты локальных сетей от несанкционированных воздействий со стороны открытых коммуникаций, базовые протоколы и средства построения защищенных виртуальных сетей на различных уровнях сетевого взаимодействия. Разрабатываются современные стандарты, протоколы и средства, используемые для обеспечения безопасности глобальных сетевых технологий.

Уже значительное время ведется работа по усовершенствованию базовых протоколов и внедрению их в существующие системы передачи информации. Широко используемое семейство протоколов TCP/IP разрабатывалось в качестве основы информационного взаимодействия более четверти века назад, вследствие этого основные концепции протоколов не соответствуют современному представлению о безопасности и защите информации от несанкционированного доступа.

Одним из самых мощных средств обеспечения безопасности служит технология преобразования сетевых адресов (Network Address Translation, сокращенно NAT). NAT представляет собой предварительный стандарт Интернет-протокола, применяемый с тем, чтобы «спрятать» истинные адреса частной сети за одним или несколькими выделенными адресами. Механизм преобразования сетевых адресов (NAT) позволяет подключать локальную сеть к Инетрнет через единственный адрес IP, при этом все компьютеры локальной сети работают так, как если бы каждый из них был подключен к Интернет напрямую.

Сферы применения технологии NAT весьма разнообразны, однако главная задача заключается в создании почти неограниченного адресного пространства внутри локальных сетей, которое «преобразуется» таким образом, что при установке двусторонней связи с общедоступными сетями обеспечивается полная защита информации о чувствительных узлах локальных систем. Тем самым, не обладая сведениями о закрытом адресном пространстве внутреннего интерфейса, становится практически невозможным атаковать напрямую тот или иной узел внутренней сети, защищенной технологией NAT .

В нашей стране накоплен значительный опыт разработки защищенных информационных систем, причем не только государственных и не только закрытых. Разработаны и успешно применяются криптографические и системно-технические методы защиты информационных технологий, в том числе, интернет-технологий. Имеется значительное число сертифицированных средств защиты информации. Все это позволяет создавать полнофункциональные системы защиты информационных ресурсов. При этом следует иметь в виду, что за состоянием защищенности информации должен осуществляться постоянный контроль, а сами средства защиты должны постоянно совершенствоваться ввиду развития методов и средств нападения на информационные ресурсы.

Поэтому одним из главных компонентов системы обеспечения безопасности киберпространства России должен стать постоянный мониторинг уровня защищенности сегментов ее информационного пространства, а также создание служб по ликвидации последствий чрезвычайных ситуаций в информационной сфере. На основании результатов мониторинга можно заранее выявлять уязвимые места в информационной инфраструктуре страны и принимать упреждающие меры по недопущению чрезвычайных ситуаций, в частности, путем организации антивирусной защиты информационно-телекоммуникационных систем. В этом направлении уже сделаны определенные шаги. В ФСБ России начал функционировать Антивирусный центр, главными задачами которого являются оценка качества антивирусных средств и обновлений к ним, выработка рекомендаций по построению антивирусной защиты информационно-телекоммуникационных систем органов государственной власти России, оказание помощи при ликвидации последствий заражений, оценки уровня защищенности систем.

Наконец, для обеспечения безопасности информационных ресурсов необходимо постоянное повышение уровня образования пользователей в области информатики, повышение квалификации разработчиков, экспертов и обслуживающего персонала информационных систем. Достаточная квалификация персонала и своевременное ее повышение является сравнительно недорогим средством повышения безопасности информационного пространства. В нашей стране сложилась система подготовки и переподготовки специалистов в области информационной безопасности. Учебно-методическое объединение по этой специальности, возглавляемое ИКСИ Академии ФСБ, объединяет более 75 вузов России.

## Заключение

Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Предотвращение несанкционированного доступа к конфиденциальной информации, циркулирующей в телекоммуникационных сетях государственного и военного управления, к информации национальных и международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью и международным терроризмом, а также в банковских сетях является важной задачей обеспечения безопасности глобальной информации.

## Литература

1. Баяндин Н.И. Технологии безопасности бизнеса. Введение в конкурентную разведку. – М.: Юристъ, 2002. – 320 с.
2. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. – СПб.: BHV, 2000. – 320 с.
3. Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. – М.: Фонд «Университет», 2000. – 428 с.
4. Партыка Т. Л., Попов И. И. Информационная безопасность. – М.: Инфра-М, 2002. – 368 с.
5. Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь, 2003.
6. Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России. – М.: Экзамен, 2003.
7. Шахраманьян М.А. Новые информационные технологии в задачах обеспечения национальной безопасности России. – М.: ФЦ ВНИИ ГОЧС, 2003.
8. Швец Д.Ю. Информационная безопасность России и современные международные отношения. – М., 2001.
9. Ярочкин В.И. Информационная безопасность. Учебник для вузов. – М.: Академический Проект, Мир, 2004. – 544 с.