DOI: 10.17117/na.2015.08.774

Поступила (Received): 20.08.2015

<http://ucom.ru/doc/na.2015.08.774.pdf>

Жумадилова Ж.Б., Жумадилова М.Б. К вопросу безопасности компьютерных сетей

Zhumadilova M.B., Zhumadilova Zh.B.
On the question of security of computer networks

Возрастающая роль информационной безопасности в сфере компьютерных сетей, в том числе и в глобальной, обуславливает необходимость расширения научных исследований не только в рамках информационной безопасности компьютерных сетей, но и в области ее инфраструктуры

Ключевые слова: информационная безопасность, компьютерные системы, защита информации

The increasing role of information security in the sphere of computer networks including in global, causes need of expansion of scientific researches not only within information security of computer networks, but also in the field of its infrastructure

Key words: information security, computer systems, information security

Жумадилова Жаркын Бапановна

Кандидат физико-математических наук, доцент
Казахский гуманитарно-юридический университет
г. Астана, Кургальджинское шоссе, 8

Zhumadilova Zharkyn Bapanovna

Candidate of Physico-mathematical Sciences,
Associate Professor
Kazakh humanitarian law university
Astana, Korqalzhyn highway, 8

Жумадилова Мереке Бапановна

Кандидат технических наук, профессор
Каспийский государственный университет
технологий и инжиниринга им. Ш. Есенова
г. Актау, 32 микрорайон

Zhumadilova Mereke Bapanovna

Candidate of Engineering Sciences, Professor
Caspian state university of technologies and
engineering named Sh. Esenova
Aktau, 32 dist.

Возрастающая роль информационной безопасности в сфере компьютерных сетей, в том числе и в глобальной, обуславливает необходимость расширения научных исследований не только в рамках информационной безопасности компьютерных сетей, но и в области ее инфраструктуры.

Зарубежные исследователи компьютерных технологий активно изучают угрозы компьютерным системам с электронными информационными инфраструктурами. В Казахстане этому вопросу уделяют значительно меньше внимания, что повышает актуальность исследований. Последнее десятилетие в Республике Казахстан увеличилась доля пользователей, использующих электронный документооборот, и с каждым годом она возрастает.

Поэтому следует ставить в приоритетные направления исследования следующие вопросы:

Обоснование и разработка ряда методологических и методических положений по определению приоритетных направлений организации информаци-

онной безопасности компьютерных сетей и их информационной инфраструктуре.

Изучение методов и систематизация современных информационных угроз применительно к компьютерным сетям и их информационной инфраструктуре.

Проведение системного анализа безопасности компьютерных сетей.

Особенности обеспечения информационной безопасности компьютерной сети заключаются в том, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений.

Рассмотрим ситуации, с которыми может столкнуться пользователь в том случае, если он подозревает, что его компьютер поражен вирусом, но ни одна из известных антивирусных программ не дает положительного результата.

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих "информационной безопасности":

- целостности данных;
- конфиденциальности данных;
- доступности данных.

Целостность данных – одна из основных целей информационной безопасности сетей – предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связана с невозможностью реализации этих функций.

В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную связанность;
- разнородность корпоративных информационных систем;
- распространение технологии "клиент/сервер".

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.

Использования технологии "клиент/сервер" с точки зрения информационной безопасности имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому.

Список используемых источников:

1. Абдикеев Н.М. Интеллектуальные информационные системы. М.: КОС-ИНФ, Рос. экон. акад., 2003. 188 с.
2. Петров В.Н. Информационные системы. СПб: Питер, 2003. 687с.
3. Хоффман Л. Современные защиты информации. М.: Сов. Радио, 1980.
4. Мамиконов А.Г. Проектирование АСУ. М.: Высшая школа, 1987.
5. Мельников В. Защита информации в компьютерных системах. М.: Электроинформ, 1997.
6. Раторгуев С.П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1995.
7. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. БЧИ-Петербург. 2002.
8. Спесивцев А.В. Защита информации в персональных ЭВМ.
9. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1995.

10. Ростовцев А.Г., Матвеев В.А. Защита информации в компьютерных системах. Вып. 2: Элементы криптологии. Санкт-Петербург: СПбГТУ, 1993.
11. Яценко В.В. Введение в криптографию. МЦНМО, 2001.
12. Жумадилова М.Б. Теоретические основы криптографии. Актау: Актау-Принт, 2012.

© 2015, Жумадилова Ж.Б., Жумадилова М.Б.
К вопросу безопасности компьютерных сетей

© 2015, Zhumadilova M.B., Zhumadilova Zh.B.
On the question of security of computer networks