ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННЫМ СРЕДСТВАМ ДЕЗОРГАНИЗАЦИИ ОБЩЕСТВА

ЭБИМОГХАН ТАРИЕБИ МАРШАЛ, Л.М. ЛЫНЬКОВ А.М. ПРУДНИК

Рассматриваются информационные средства дезорганизации общества, которые основываются на идеях теории сетевых войн. Показано, что данная теория распространяется путем управляемого воздействия на бытовую, общественно-политическую, энергетическую, военно-стратегическую и другие составляющие обеспечения жизнедеятельности государств. Такие сети состоят собой из средств связи, масс-медиа, транснациональных корпораций, политических и религиозных организаций, специальных служб. Особенностью сетевых войн является принцип неразрывности идеологии и технологии для осуществления контроля мировой общественно-политической ситуации.

Представлен обзор современных методов и средств для управляемого воздействия страны в аудио- и телекоммуникационных системах, предложены методы и приемы по снижению энергоинформационных, социально-информационных опасностей и угроз.

Предложены способы снижения уровня воздействия негативных информационных факторов на население страны путем противодействия угрозам таким воздействий и организации контроля. Показано, что основное проявление результатов информационного воздействия происходит при различных внештатных и чрезвычайных ситуациях.

Выявлены возможные угрозы нейролингвистического программирования населения через различные средства телекоммуникаций и разработке комплекса рекомендаций по снижению последствий таких воздействий. Разработаны возможные приемы защиты от подпороговой информации, влияющей на поведение человека при внештатных и чрезвычайных ситуациях.

ИССЛЕДОВАНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ ПРОДУКТОВ

В.В. МАЛИКОВ, И.В. БЕНЕДИКТОВИЧ, С.А. ЧУРЮКАНОВ

В настоящее время проведена оценка статистических данных по уязвимостям, выявленным в программных продуктах специализированными компьютерными группами реагирования на чрезвычайные ситуации.

Основные результаты проведенной экспертной оценки:

1. Наибольшее количество уязвимостей с 1999 г. по 2014 г. выявлено в программных продуктах вендоров: Microsoft (374 продукта / 3377 уязвимостей, из них 35% критических), Oracle (241 продукт / 2257 уязвимостей, из них 18% критических), Apple (100 продуктов / 2225 уязвимостей, из них 24% критических). Microsoft за январь–апрель 2014 г. было опубликовано 20 бюллетеней безопасности.

2. Наиболее уязвимыми программными продуктами с 1999 г. по 2014 г. являлись: Linux Kernel (Linux, 1146 уязвимостей, из них 2% критических), Firefox (Mozilla, 1067 уязвимостей, из них 41% критических), Chrome (Google, 941 уязвимость, из них 18% критических). Так в версии Chrome 1.0.154.53 было выявлено 514 уязвимостей.

3. Основные типы уязвимостей с 1999 г. по 2014 г.: Execute Code — 32,9%, DoS — 21,1%, Overflow — 14,8%.

4. Пиковые значения выявленных уязвимостей пришлись на 2006–2007 гг. (6610 шт. и 6520 шт. соответственно).

5. US-CERT в качестве основных атак/уязвимостей за январь–апрель 2014 г. определил следующие: OpenSSL «Heartbleed» уязвимость (TA14-098A / CVE-2014-0160), Microsoft Ending Support for Windows XP and Office 2003 (TA14-069A), UDP-based

Amplification Attacks (TA14-017A), NTP Amplification Attacks Using (TA14-013A / CVE-2013-5211), Malware Targeting Point of Sale Systems (TA14-002A).

6. National Vulnerability Database NIST по состоянию на апрель 2014 г. включает 62020 актуальных уязвимостей.

Таким образом, своевременная оценка уязвимостей позволяет повысить эффективность реагирования на инциденты информационной безопасности, а также обеспечить гарантированную защиту объектов различных категорий.

ОЦЕНКА КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ

Н.В. МИНОВ

Криптографическая стойкость — свойство криптографического шифра противостоять криптоанализу, то есть анализу, направленному на изучение шифра с целью его дешифрования. Криптостойкость шифра есть его важнейшая характеристика, которая отражает меру устойчивости системы к атакам. Система называется стойкой, если злоумышленник не может взламывать ее слишком часто или слишком быстро. Для измерения стойкости алгоритма необходимо оценивать вероятность взлома и объем вычислительных задач [1].

Стойкость абсолютно стойких алгоритмов не зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическое применение систем, удовлетворяющих требованиям абсолютной стойкости, ограничено соображениями стоимости.

Определены следующие требования к такого рода шифрам: каждый ключ используется только один раз, все ключи равновероятны, длина ключа равна или больше длинны сообщения [2].

В основном в криптографических алгоритмах применяются вычислительно стойкие системы. Стойкость этих систем зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическая стойкость таких систем оценивается последовательно с двух позиций: вычислительная сложность полного перебора, известные уязвимости системы и их влияние на вычислительную сложность.

Литература

1. *Венбо М.* Современная криптография. Теория и практика. М., 2005.

2. *Шеннон К.* Теория связи в секретных системах. [Электронный ресурс]. — Режим доступа: http://www.enlight.ru/crypto/articles/shannon. — Дата доступа: 23.04.2014.

ЗАЩИТА ЧЕЛОВЕКА ОТ ВЛИЯНИЯ АКУСТИЧЕСКИХ ВОЛН РАЗЛИЧНЫХ ДИАПАЗОНОВ

В.В. МИРОНЧИК

В современном мире человек постоянно воспринимает информацию по акустическому каналу. Воздействовать на психоэмоциональное состояние человека можно с помощью звуковых волн различных частот.

При воздействии на человека частотами, относящимися к инфразвуку (область частот ниже 20 Гц) и ультразвуку (частоты свыше 20 кГц), человеческое ухо не воспринимает какую-либо информацию, но вызываются резонансные явления всего тела человека. Данные резонансные явления в зависимости от их интенсивности и продолжительности могут вызывать различные нарушения в организме человека. Для защиты от данного типа воздействий на различных производствах необходимо использовать звукопоглощающие камеры, не передающие вибрации, расположенные на определенном удалении от источника данных частот.