потенциальных проблем в будущем, но и сэкономить достаточно большие средства, что в первую очередь важно для бизнеса.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ И ПРОГРАММНАЯ ЗАЩИТА ИНФОРМАЦИИ

А.Н. Макаров, Ю.А. Скудняков

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты для исполнения своих противоправных интересов и получения конфиденциальной информации. Все средства инженерно-технической защиты применяются для различных объектов взаимодействия: людей, информации, финансовых и материальных средств. По назначению средства инженерно-технической защиты делятся на группы: 1) физические средства включают различные средства и сооружения, которые могут препятствовать физическому проникновению или доступу злоумышленников на объекты защиты, к материальным носителям конфиденциальной информации, и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий; 2) аппаратные средства, в которые входит оборудование, содержащее различные приборы, приспособления и устройства, выполняющее функцию защиты информации. На любом предприятии применяется различная аппаратура и системы, которые обеспечивают производственную деятельность. Основной задачей аппаратных средств является обеспечение надежной и уверенной защиты от утечки информации и несанкционированного доступа к ней через технические средства, находящиеся на предприятии; 3) криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования [1]; 4) программные средства, которые охватывают специальные программы и комплексы, а также информационные системы обработки данных, включающие в себя защиту информации. Приведенные выше средства инженерно-технической и программной защиты являются базовыми для обеспечения защиты информации. В современном мире информационное поле становится основой взаимодействия внутри и между объектами и имеет глобальный доступ по всему миру. Средства защиты находятся в постоянном совершенствовании и развитии для предотвращения доступа в исполнении противоправных действий. Исходя из вышеизложенного, авторами работы разработана система защиты, алгоритм функционирования которой постоянно изменяется и совершенствуется. Только комплексное использование всех групп инженерно-технической и программной защиты позволяет предотвратить несанкционированный доступ к защищаемой информации.

Литература

1. Партыка Т.Л., Попов И.И. Информационная безопасность. М.: ФОРУМ: ИНФРА-М., 2005. 243 с.

ТЕСТИРОВАНИЕ СЕТЕВЫХ РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, М.А. Бабич, В.Н. Ярошевич

Исследован уровень информационной безопасности (ИБ) сервисов/ресурсов в сети интернет на примере кредитно-финансовых организаций (КФО) Республики Беларусь. Для проведения исследования были выбраны 25 белорусских КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности.

На основании проведенного тестирования можно сделать следующие выводы:

1. Наиболее часто используемые AS для КФО: ASN 12406 (ООО «Деловая сеть») – 7 сетевых ресурсов, ASN 6697 (РУП «Белтелеком») – 5 сетевых ресурсов.

2. Структура сервисов/ресурсов ДБО КФО, как правило, имеет уязвимости:

– только 7 (35 %) из 20 КФО не имеют в своей структуре уязвимых referrer-файлов;