существующей политики обеспечения ИБ на предмет полноты и эффективности; моделирование возможных действий нарушителей ИБ; построение дерева угроз ресурсам ИС, а также дерева недостатков существующей системы; анализ экономических, информационных и технических рисков связанных с осуществлением угроз ИБ; разработка тестовых моделей оценки устойчивости СИБ и ее компонентов; формирование рекомендаций по разработке (или доработке) стратегии обеспечения ИБ; формирование предложений по использованию существующих и установке дополнительных средств защиты информации для повышения уровня надежности СИБ.

Литература

1. Жук О.Ю. // Архивы и делопроизводство. 2008. № 3. С. 123–128.

НЕКОТОРЫЕ ОСОБЕННОСТИ СИНТЕЗА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Федорцов

Известно, что источником реальной угрозы для безопасности информации, обрабатываемой в информационной системе (ИС), и эксплуатируемых программно-технических комплексов являются, прежде всего, субъекты информационных отношений (пользователи), реализующие право на использование информации и элементов ИС [1]. Также негативное воздействие на защищаемые объекты и информацию, используемую технику защиты могут оказывать включенные в состав системы защиты информации (СЗИ) органы и (или) исполнители [2]. Полностью нейтрализовать указанные угрозы не представляется возможным. Из-за допущенных ошибок при проектировании, существующие СЗИ способны лишь отчасти снизить величину ущерба, который может быть нанесен оператору (владельцу) ИС мотивированными злоумышленниками (инсайдерами), а также другие риски от их действий. Следует отметить, что построение СЗИ, предполагающей оптимальное сочетание механизмов обеспечения защиты и механизмов управления ими, невозможно без соблюдения таких принципов, как: необходимость, достаточность, экономическая целесообразность и т.п. При этом, комплексный анализ рисков и формулирование требований к СЗИ должны быть тесно связаны с реальной оценкой предполагаемого ущерба от деструктивного влияния внутренних нарушителей на элементы ИС (СЗИ) и обрабатываемую информацию. Таким образом, в настоящее время исследования процесса оценки ущерба являются актуальными и имеющими практическую значимость, разработка и применение общепринятой методики такой оценки будет способствовать созданию более эффективных СЗИ.

Литература

1. Об информации, информатизации и защите информации, Закон Респ. Беларусь от 10.11.2008 № 455-З, с изменениями и дополнениями от 4 января 2014 г.

2. Защита информации. Основные термины и определения. СТБ ГОСТ Р 50922-2000: Введ. 22.05.2000 – Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. – 6 с.

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ПОПУЛЯРНЫХ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ ВЕБ-САЙТОВ

А.С. Цалко, П.В. Кучинский

Исследована безопасность веб-сайтов, написанных на скриптовом языке PHP и обслуживаемых ЦИИР БГУИР. Был проведен поиск вредоносного ПО методами сигнатурного сканирования и эвристического анализа исходных файлов веб-сайтов. В результате на небольшом количестве сайтов (менее 50) было найдено более 200 образцов вредоносного программного обеспечения.

В абсолютном большинстве доступ был получен злоумышленниками через популярные системы управления содержимым сайтов. Например, через сторонние модули CMS WordPress, на котором из 10 млн крупнейших сайтов мира в 2016 г. работают 26,2% [1]. Веб-сайты, разработанные ЦИИР БГУИР не были скомпрометированы. Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт.

Использование всех базовых и популярных методов (сложные пароли, ограничение прав на запись, регулярное обновление CMS и модулей и др.) позволило снизить уровень успешных атак, но не обеспечило полную безопасность веб-сайтов. Максимально эффективным средством является использование систем обнаружения вторжений (IDS).

Для серверов ЦИИР БГУИР, обеспечивающих работу PHP-сайтов была выбрана система OSSEC — хостовая система обнаружения вторжений (Open Source Host-based Intrusion Detection System) [2]. Данная система обладает открытым исходным кодом. С ее помощью были решены задачи проверки контроля целостности файлов, логирования различных действий на серверах, получения событий безопасности (анализ системных журналов) и оповещений об этих событиях.

В результате всех описанных методов и средств удалось существенно повысить безопасность сайтов, использующих популярные системы управления содержимым. Количество успешных сетевых атак злоумышленников значительно снизилось: на том же количестве сайтов за месяц наблюдения не было выявлено успешных атак. Проведенная работа подтверждает актуальность выбранного направления исследования информационной безопасности веб-узлов.

Литература

1. W3Techs, Software Quality Management Consulting: [Электронный ресурс]. Режим доступа: http://w3techs.com/technologies/overview/content_management/all (Дата обращения: 23.04.2016).

2. Wikipedia, OSSEC [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/OSSEC (Дата обращения: 26.04.2016).