Литература

1. *Беляцкая Т.Н.* Электронная экономика: генезис и развитие — Saarbruecken (Germany): LAP LAMBERT Academic Publishing, 2014.

2. *Ситнов А.А.* Особенности аудита электронного бизнеса // Аудитор, № 7, 2013.

ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ИНВЕСТИЦИЙ В СИСТЕМУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ СФЕРЫ ЭЛЕКТРОННОГО БИЗНЕСА

Л.М. Лыньков, В.С. Князькова

Для организаций сферы электронного бизнеса вопросы информационной безопасности являются критически важными для достижения устойчивого конкурентного преимущества и закрепления рыночного успеха.

Экономическая эффективность в общем виде определяется соотношением полученных результатов (прибыли, высвобожденные средства) к затратам (инвестициям).

Эффективность инвестиций в систему информационной безопасности (помимо классических экономический показателей оценки инвестиционных проектов, таких как коэффициент рентабельности инвестиций (ROI), чистая текущая стоимость (NPV), внутренняя норма рентабельности (IRR), период окупаемости (PP)) может оцениваться на основании следующих методик.

1. BCP (Business Continuity Management — планирование непрерывности бизнеса — это комплекс различных мероприятий, направленных на снижение рисков прерывания бизнеса и их негативных последствий.

2. Сбалансированная система показателей (Balanced Scorecard) — это система, предложенная Р. Нортоном и Д. Капланом для всесторонней оценки деятельности организации. С точки зрения информационной безопасности данная система позволяет выявить существующие взаимосвязи между важнейшими ее показателями и выявить структурные взаимосвязи.

3. TCO (Total Cost of Ownership — совокупная стоимость владения) — полный комплекс затрат, связанных с приобретением, внедрением и использованием системы и воспринимаемых как единые затраты на информационную систему в процессе её создания и эксплуатации. Чаще всего под показателем TCO понимают прямые и косвенные затраты на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года.

Таким образом, использование данных методик позволяет определить экономическую эффективность инвестиций в систему информационной безопасности организаций электронного бизнеса.

Литература

1. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. Сер.: Экономика. 2011, № 1.

АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Р.М. Михлюк

Аудит информационной безопасности проводится с целью оценки качественной и количественной составляющих состояния информационной безопасности и разработки рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и иных ресурсов информационной системы от угроз информационной безопасности. Аудит информационной безопасности является начальным этапом работ по созданию комплексной системы информационной безопасности (СИБ), который представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов от угроз информационной безопасности, связанных с нарушением доступности, целостности и конфиденциальности хранимой и обрабатываемой информации. Меры защиты организационного уровня реализуются путем проведения мероприятий, документально оформленной стратегией обеспечения информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программных, технических и программно-технических средств защиты.

В число задач, решаемых при проведении аудита, входят: сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ; анализ

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).