объектов защиты (ОЗ), а также вскрытие возможных каналов утечки информации от этих объектов. Качественное проведение мероприятий КТК призвано обеспечить оценку эффективности проводимых в войсках мероприятий маскировки и ПД ТСР противника, выполнение которых оказывает существенное влияние на снижение вероятности обнаружения противником ОЗ и получения им достоверной информации о составе, положении, состоянии, предназначении и характере деятельности войск (сил), а также замысле предстоящих действий.

Для выполнения мероприятий КТК создаются специально подготовленные подразделения КТК, основной задачей которых является проведение КТК на всех ОЗ.

В предлагаемой методике обоснования количества подразделений КТК используется математическая модель определения оптимальных маршрутов движения данных подразделений, перемещаясь по которым они смогут осуществить мероприятия КТК с заданным эффектом. Данная методика позволит должностному лицу, принимающему решение по применению подразделений КТК, равномерно распределить между ними нагрузку и назначить каждому подразделению свой район КТК.

Литература

1. Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ ред. М.П. Сычева. М. : Изд-во МГТУ им. Н.Э. Баумана, 2011. 478 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БИЗНЕСА

В.С. Князькова

Электронный бизнес (ЭБ) — вид предпринимательской деятельности, основанной преимущественно на интернет-технологиях. Интернет предоставляет огромные возможности для выстраивания различных бизнес-процессов, но, как следствие, влечет за собой дополнительные к традиционным видам деятельности риски.

Для построения модели угроз организации ЭБ необходимо определить уровень интеграции ЭБ в бизнес-процессы организации. Он может быть различным. Так, с помощью интернет-технологий организация может:

– предоставлять сведения об организации и основных видах ее деятельности (например, сайт-визитка);

– реализовывать часть бизнес-процессов посредством интернет-технологий (например, интернет-магазин для промышленного предприятия);

– выносить большинство бизнес-процессов в среду ЭБ (например, маркетинг и/или финансы, и/или логистика, и/или оказание услуг);

– реализовывать все свои бизнес-процессы в среде ЭБ (например, новостной портал).

– типичными для всех уровней интеграции ЭБ будут следующие угрозы:

– угроза потери целостности информации о бизнес-процессах и бизнес-операциях;

– угрозы вирусной атаки и подверженность мошенничеству со стороны потребителей и иных лиц посредством несанкционированного доступа к информации;

– несоблюдение требований нормативно-правового регулирования финансово-хозяйственной деятельности и, в частности, ЭБ из-за отсутствия четко выработанной законодательной системы в этой сфере;

– сбой или отказ систем и элементов информационных инфраструктур.

Дальнейший и бурный рост числа экономических субъектов, внедряющих современные информационные технологии или полностью ориентированных на электронный бизнес, обусловлен, прежде всего, тем, что при ведении финансово-хозяйственной деятельности в современной электронной среде значительно снижаются транзакционные издержки, т.е. издержки, сопряженные с переходом прав собственности на потребительский результат.

Обычно руководство и лица, наделенные руководящими полномочиями экономического субъекта, вовлеченного в электронный бизнес, оценивают бизнес- и ИТ-риски посредством внедрения системы информационной безопасности, создания надлежащей ее инфраструктуры и применения надлежащих средств контроля, которые направлены:

– на идентификацию и проверку подлинности потребителей и поставщиков;

– на обеспечение целостности информации о бизнес-операциях;

– на получение оплаты или обеспечения в отношении кредитных средств потребителей;

– на установку протоколов конфиденциальности и защиты информации.

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