грамм в области ИБ, в противовес им 77% наоборот намерены увеличивать затраты.

Несмотря на это, следует отметить, что многие компании будут заинтересованы в аудите ИБ, так как зачастую руководству компаний требуется независимая оценка состояния ИБ, деятельности служб ИБ и проектов в данной области.

Список нормативной и научной литературы:

1. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.
2. ISO/IEC 27000 – Семейство Международных Стандартов Управления Информационной Безопасностью.
3. www.crime-research.md.
4. www.itsec.ru.

Лилия Павлова,
компания IT&IS Management SRL

УПРАВЛЕНИЕ РИСКАМИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В настоящее время информационные технологии (ИТ) значительно расширили возможности для ведения бизнеса. Высокие технологии позволяют не только повысить эффективность бизнес-процессов, но и могут стать источником колоссального ущерба. Утечка конфиденциальных данных, вирусы, хакеры, спам – данных проблем почти невозможно избежать, так как их существование обусловлено применением ИТ в бизнесе. Тем не менее, ИТ-рисками можно управлять.

Управление ИТ-рисками становится все более значимым разделом общей системы Управления Рисками. Меры по анализу и минимизации ИТ-рисков составляют предмет отдельной дисциплины – управление информационно-технологическими рисками (Information Technology Risk Management – ITRM).

Управление ИТ-рисками состоит из их периодической оценки и выполнения мероприятий по снижению выявленных рисков до приемлемого уровня. Данный процесс включает в себя управление рисками безопасности, доступности, производительности и согласованности.

Для управления ИТ-рисками необходимо применять:

- методики, учитывающие положения и требования международных стандартов ISO/IEC 17799, BS7799, ISO/IEC 27001;
- CobiT (Control Objectives for Information and related Technology);
- рекомендации NIST (National Institute of Standards and Tech-

nology), в частности NIST SP800-30 Risk Management Guide for Information Technology Systems;
- закон Сарбейнса-Оксли.

В результате опроса, проведенного аналитической компанией Freeform Dynamics, среди 715 руководителей ИТ-отделов в странах Европы и Ближнего востока, стало очевидно, что, несмотря на все более качественную оценку рисков и улучшенное планирование деятельности по их предотвращению, многие компании все еще не имеют интегрированной стратегии управления ИТ-рисками.

Исследование показало, что одна из главных причин отказа от внедрения новых технологий, необходимых для создания конкурентных преимуществ, развития бизнеса и обеспечения соответствия нормативным требованиям, – постоянные опасения по поводу ИТ-безопасности и неуверенность, что та и ли иная технология может быть интегрирована с системами хранения и восстановления данных компании.

Эффективное управление ИТ-рисками является обязательной частью бизнеса, существующей для того, чтобы при возникновении рисков в области ИТ реагировать на них должным образом, управлять ими, измерять, контролировать и поддерживать информированность о них.

Структура и процессы управления ИТ-рисками должны обеспечивать точность, конфиденциальность, доступность, безопасность и скорость передачи информации, которая создается, обрабатывается и распространяется внутри компании и между клиентами. Несоблюдение одного или всех этих условий может серьезно отразиться на репутации или финансовом состоянии компании.

Процессы управления ИТ-рисками следующие:

1. Инвентаризация информационных активов и оценка их критичности;
2. Идентификация угроз и уязвимостей;
3. Определение вероятностей и воздействий;
4. Анализ угроз и уязвимостей;
5. Определение рисков;
6. Анализ рисков;
7. Выбор приоритетных для защиты активов и утверждение плана мероприятий по их защите;
8. Оценка и контроль рисков.

В процессе инвентаризации информационных активов должен быть составлен общий макет информационной инфраструктуры компании. В этом аспекте в раздел информационных активов будут входить: информационные ресурсы, программное обеспечение, материальные активы и услуги.

Анализ рисков – составная часть управления информационными рисками, в процессе которого оцениваются уязвимости информационной инфраструктуры компании к угрозам безопасности, их критичность и вероятность ущерба, вырабатываются контрмеры по уменьшению рисков до приемлемого уровня и обеспечивается контроль защиты информационной инфраструктуры.

Самыми популярными методиками анализа рисков являются американская методика Carnegie Mellon's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) Security Risk Evaluation и английская методика Commercial Risk Analysis and Management Methodology (CRAMM).

Оценивая риски, ИТ-специалисты не ограничиваются лишь одними информационными системами, программным, аппаратным и коммуникационным обеспечением, а рассматривают также вопросы физической безопасности и учитывают человеческий фактор.

Оценку ИТ-рисков следует проводить не реже двух раз в год, чтобы можно было гарантировать, что не остались невыявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно.

Внутри организации работа по оценке рисков должна быть нормализована путем формирования соответствующей политики, создания стандартов и руководств.

Эффективные процессы управления ИТ-рисками сокращают затраты и могут повысить валовой доход. От процессов управления ИТ-рисками может быть получена значительная прямая экономия затрат, отражающаяся на чистой прибыли, в долгосрочной перспективе гораздо более ценными. В целом будет повышение валового дохода, как следствие своевременного оповещения о рисках, стратегические инвестиции и улучшение производительности.

Список нормативной и научной литературы:

1. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.
2. NIST 800-30:2002 Руководство по управлению рисками для ИТ-систем.
3. COBIT Контрольные объекты для информационных и смежных технологий.

Олег Солоненко,
S&T Mold

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

This article describes how to assess the cost-effectiveness of information security through methodologies ROI, TCO, as well as the possibility of applying a set of methods to assess a number of financial and non-financial indicators such as KPI and BSC.

Информационная безопасность – есть *процесс*, направленный на достижение состояния защищённости информационной среды: устройств, процессов, программ, и данных, обеспечивающий конфиденциальность, целостность и доступность информации, которая обрабатывается, хранится и передается в этой среде.

Классической оценкой эффективности информационной безопасности является аудит на соответствие