УДК 65.012.123

РАЗРАБОТКА ПРОГРАММЫ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

В.А. ВЛАСЕНКО, С.Л. ПРИЩЕПА

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 5 марта 2015

В условиях постоянного развития информационных технологий вопрос эффективного управления информационной безопасностью становится все более актуальным. В данной статье рассматривается пошаговая разработка программы безопасности коммерческого предприятия, позволяющей экономически грамотно обрабатывать информационные риски организации. Обращается внимание на важные организационные особенности, которые необходимо учитывать при построении документов по безопасности для их качественного внедрения и постоянного поддержания в актуальном состоянии.

Ключевые слова: программа безопасности, стратегическое планирование, управление рисками, система управления информационной безопасностью, контроль изменений.

Введение

В настоящее время состояние глобальной экономики заставляет компании считаться с рисками и вести постоянную работу по разработке более эффективных механизмов управления. Одной из фундаментальных моделей внутреннего контроля корпоративного управления является ERM COSO [1] (Committee of Sponsoring Organizations of the Treadway Commission). Его структуры придерживаются многие ведущие мировые компании.

Анализируя стандарты корпоративного управления и качества, можно выделить несколько основных этапов зрелости предприятий в соответствии со стоящими перед ними приоритетами и провести аналогию с резким ростом информатизации в обществе, а соответственно и сделать вывод о причинах изменения стандартов в области безопасности. Большинство компаний, находясь на втором этапе зрелости, проявляли повышенный интерес к информационным технологиям как к средству повышения эффективности технологических процессов и их оптимизации. Сейчас мы можем наблюдать тенденцию стремительного развития области безопасности, которая, в первую очередь, связана с повышенным вниманием инвесторов к безопасности, а именно: к проблематике риска менеджмента, постоянно изменяющимся требованиям к организации защиты критических коммерческих данных.

Границы области безопасности точно очертить невозможно, безопасность охватывает все новые аспекты деятельности предприятий. Специалисты, работающие в данной области, всегда испытывали трудности при описании этого понятия. Только в сфере компьютерных технологий, безопасность касается разработки программного обеспечения – компьютерная безопасность призвана гарантировать, что программное и аппаратное обеспечение удовлетворяет своим спецификациям и требованиям при использовании его в потенциально враждебной среде [2]. Включая вопросы спецификации, валидации, верификации, тестирования, надежности компьютерной системы. Безопасность охватывает гораздо больший круг проблем, касающихся проектирования операционных систем, архитектурного проектирования, информационной безопасности, анализа и управления рисками, организации и управления базами данных, шифрования и кодирования, отказоустойчивости, проектирования интерфейсов, постановлений и политики государства, административных

решений, экономической безопасности, конкурентной разведки, компетентности в вопросах безопасности, а также соответствующего образования. В данной работе под термином «безопасность информации» будем понимать состояние, которое должны обеспечивать организационные, правовые, программно-аппаратные, инженерно-технические и силовые меры, методы и средства, направленные на обеспечение целостности, конфиденциальности, доступности информации.

Понимание проблем управления процессами безопасности подвергается качественному изменению. В первую очередь, происходящее можно связать с совокупным развитием экономики и информационных технологий. Задачи, стоящие перед безопасностью, значительно усложнились. Данный факт подтверждается многочисленными аргументами, одним из них является необходимость контроля распространения информации на любых носителях, перечень которых постоянно увеличивается. Если безопасность не интегрирована в деятельность компании, а за ее обеспечение отвечают исключительно подразделения безопасности – безопасность такой компании сужается до технических аспектов, а такой подход в данный момент является малоэффективным [3]. Потому специалисты утверждают, что важность выбора правильной стратегии развития в области и интеграция безопасности в бизнес-среду играет одну из ключевых ролей при достижении успеха и финансовой стабильности компании на сегодняшний день.

Программа безопасности

В последних исследованиях по обеспечению информационной безопасности все чаще отмечается важность учета нетехнических аспектов деятельности наравне с техническими рисками [4]. Наблюдается тенденция к интеграции процессов безопасности скорее в бизнес-среду, нежели в информационные технологии. В данный момент делается акцент на новых информационных рисках, таких как: человеческий фактор, культура безопасности, организационные нормы обеспечения безопасности, репутационные риски. Эти данные представляют определенную сложность с точки зрения управленческого учета.

Одновременно с этим присутствует острая потребность в разработке формализованных моделей управления деятельностью по обеспечению безопасности информации, которые учитывают упомянутые выше нетехнические аспекты. Таким образом, определенную актуальность представляет модель централизованного управления деятельности в области защиты информации, которая уже плотно закрепилась в европейских, американских исследованиях и стандартах. Данная концепция управления подразумевает управление нормами и ограничениями, что выглядит перспективным подходом к решению рассмотренных выше проблем.

Перед разработкой концепции рекомендуется обратить внимание на стандарты серий ISO/IEC 27000, 9000, COBIT (ISACA COBIT Framework), CISSP CBK (Common Body of Knowledge), ITIL (IT Infrastructure Library), COSO (IRM COSO Framework).

Стандарты серии ISO/IEC 2700x являются фундаментальными и близки по содержанию к CISSP CBK. Другие стандарты призваны решать наиболее актуальные проблемы в отрасли. Поскольку персонал департаментов бизнеса и IT используют различную терминологию и ставят перед собой различные цели, это может приводить к неэффективному управлению, нарушению сроков, упущенным возможностям, увеличению затрат времени и сил, разочарованиям с обеих сторон. Для решения этих целей предназначены стандарты COBIT и ITIL. Стандарт COBIT [5] определяет цели и модель управления IT. Стандарт ITIL в первую очередь указывает последовательность действий на уровне процессов, необходимых для достижения цели. ITIL был создан для удовлетворения потребностей бизнеса, в связи с его растущей зависимостью от IT. В ITIL существуют домены по безопасности, внимание которых в основном сконцентрировано на внутренних соглашениях об уровне обслуживания между IT и другими подразделениями компании, которые он обслуживает.

При разработке программы безопасности в настоящее время становится очень важным правильно определить четкие цели, достижение которых ожидается в результате выполнения программы безопасности. Наиболее правильным подходом при реализации программы

считается подход «сверху-вниз», начиная со стратегических целей и заканчивая детальными конфигурациями и системными параметрами каждого объекта окружения.

Специалисты по безопасности обязаны понимать, что безопасность должна соблюдаться в рамках всей компании и крайне важно иметь несколько центров ответственности и подотчетности. Потому первым этапом рекомендуется закрепить обязанности и ответственность по обеспечению безопасности за руководителями всех подразделений. Это позволит создать правовое поле и подготовить фундамент и соответствующую мотивирующую площадку для сторонних подразделений, вовлеченных в разработку программы безопасности. Для выполнения этого этапа необходимо также провести инвентаризацию, идентификацию, оценку активов компании. Результатом этапа будет служить матрица ответственности и определение владельцев активов. Данная модель призвана учесть все аспекты деятельности и контролировать их изменения.

Владельцы информации должны указывать, какие пользователи могут иметь доступ к их ресурсам и что они могут делать с этими ресурсами. Задача администратора безопасности – убедиться, что этот процесс внедрен. Владельцем актива информации обычно является ответственный сотрудник, входящий в руководящий состав компании или руководитель соответствующего управления. Таким образом, владелец несет единоличную ответственность за любую халатность и классификацию информации.

На втором этапе разработки важно понимать, что программа безопасности должна иметь непрерывный жизненный цикл и постоянно совершенствоваться (рис. 1).

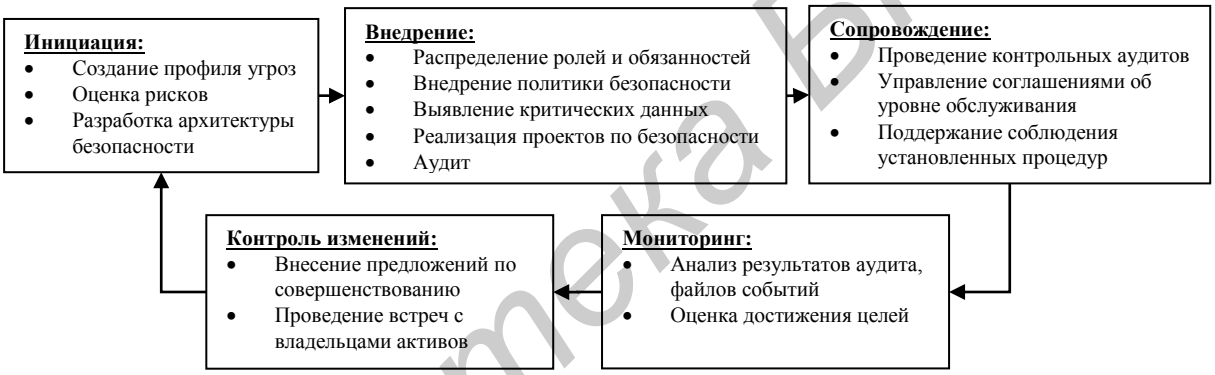

Рис. 1. Этапы разработки программы безопасности

На вышеизложенных этапах ведется подготовка правового поля для эффективного внедрения программы безопасности, назначаются ответственные. Определяются границы ответственности, обеспечивается контроль актуальности и внесения только согласованных изменений.

Основным фундаментом программы безопасности являются следующие процессы: управление рисками; управление активами; управление уязвимостями; соответствие требованиям; управление изменениями; управление идентификацией и доступом; классификация информации; планирование непрерывности бизнеса; физическая безопасность; уровни ответственности; жизненный цикл разработки программного обеспечения; обработка инцидентов; обучение персонала.

Разработка программы безопасности осуществляется в несколько шагов, фундаментом являются бизнес-процессы компании. Остановимся подробнее на некоторых более важных из них с точки зрения стратегии.

Риск – вероятность того, что источник угрозы воспользуется уязвимостью, что приведет к негативному последствию для компании. Источником угрозы может быть вирус, хакер, пользователи, сотрудники и др. Потому очень важно надлежащим образом организовать контроль и аудит действий, что позволяет значительно проще расследовать инциденты безопасности.

Управление информационными рисками представляет собой процесс обработки рисков, снижения их до приемлемого уровня, а также внедрения механизмов поддержания (рис. 2). При управлении рисками составляется перечень категорированных угроз, которые также должны быть оценены с точки зрения потенциальных потерь и вероятности возникновения. Реальные

риски чрезвычайно трудно измерить, потому специалисты рекомендуют основное внимание обратить на приоритезацию данного списка. Полноценное управление рисками требует поддержки высшего руководства, документированного процесса IRM-политики и IRM-группы. Анализ рисков обеспечивает идентификацию активов и их ценности для компании, идентификацию угроз и уязвимостей, количественную оценку вероятности и влияния на бизнес потенциальных угроз, обеспечение экономического баланса между ущербом от воздействия угроз и стоимостью контрмер. Одной из первых задач группы анализа рисков является подготовка детального отчета по стоимости активов.

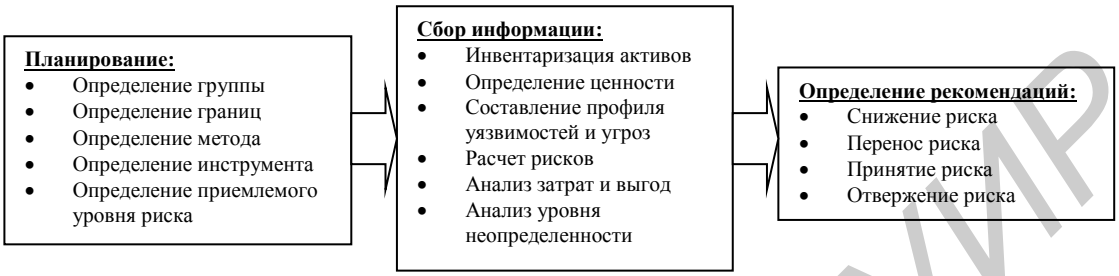

Рис. 2. Жизненный цикл программы управления рисками

Оценка стоимости активов включает в себя процесс определения текущего и желаемого состояния безопасности организации. Подход основан на оценке фактической стоимости актива, на оценке временных затрат, усилий и ресурсов, требуемых для его создания либо ущерба в случае уничтожения. Для проведения анализа рисков компания должна решить, какие активы нуждаются в защите и в какой степени. Оценивается функциональность доступных защитных средств, определяются наиболее эффективные контрмеры. Для поддержания безопасности на приемлемом уровне стоит отметить, что необходимо переоценивать риски на периодической основе.

После внедрения контрмеры компании необходимо оценить величину остаточного и общего риска, достигнутого с помощью контрмер. Разделяют несколько способов обработки рисков: перенести, избежать, уменьшить и принять.

Политика безопасности – документ, указывающий на роль безопасности в организации. Политика должна быть независимой с точки зрения технологий и решений. Должна очерчивать цель и миссию, но не привязывать компанию к способам достижения. Политики принято классифицировать по объектам назначения: организационная политика; политика, ориентированная на задачи; политика, ориентированная на системы. В первую очередь политика существует для решения задач предоставления полномочий группе безопасности и ее деятельности, является основанием в процессе разрешения конфликтов, связанных с безопасностью, очерчивает персональную ответственность, обязанности в отношении реагирования на инциденты и др.

В политике безопасности должен быть разработан и внедрен четкий и понятный порядок применения мер воздействия в отношении тех, кто не соблюдает требования политики безопасности. Политики пишутся в широких терминах и покрывают множество систем и устройств. Более детализированные документы требуют частой актуализации – процедуры, стандарты, руководства, которые составляют ее структуру [3]. А необходимые компоненты, заполняя эту структуру, обеспечивают выполнение программы безопасности и предоставляют защищенную инфраструктуру.

Классификация информации – процесс определения ценности информации для компании, который помогает определить, какие средства и меры защиты должны применяться для каждого класса, решить, какие задачи защиты информации являются наиболее приоритетными (рис. 3). Первичная задача классификации информации – показать необходимый для каждого типа информации уровень защиты конфиденциальности, целостности и доступности и сделать это наиболее эффективным способом. Как правило, в зависимости от размеров организации различают три, четыре уровня иерархии. В военных ведомствах могут использовать пять уровней иерархии.

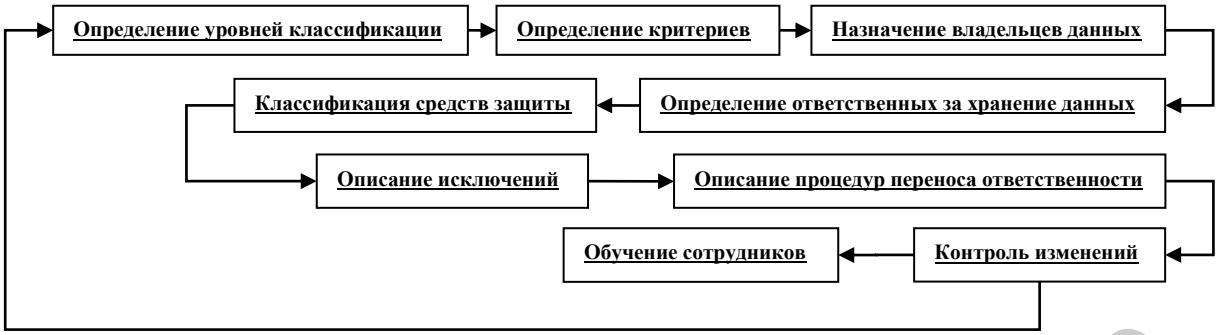

Рис. 3. Описание процесса классификации данных

Аудит информационной безопасности проводится с целью выявления пробелов в существующей системе безопасности, определении пробелов и недочетов, нуждающихся в улучшении или корректировке, а также определение необходимых ресурсов, требуемых для достижения конечной цели безопасности. Это можно обеспечить с помощью создания структуры безопасности, состоящей из нескольких уровней: функций безопасности; обеспечения безопасности мероприятий и процессов, необходимых для реализации каждой из них и возможностей безопасности, связанной с деятельностью по безопасности.

Заключение

В данной статье проведен выборочный анализ некоторых международных стандартов по информационной безопасности и сделана попытка систематизации полученных знаний с последующим выделением ключевых особенностей, требующих особого внимания на начальных этапах внедрения методологической базы в области безопасности. Проведен анализ корреляционных связей между программой безопасности и бизнес-целями компании. Приведены шаги, необходимые для создания эффективной программы безопасности на всех уровнях коммерческой организации. Показана актуальность проблем, стоящих перед информационной безопасностью, которые можно решить с помощью разработки стратегии безопасности. Программа безопасности в состоянии значительно снизить информационные риски организации и привести к эффективному управлению. Данная программа должна быть актуальной на всех уровнях организации, а также пересматриваться в связи с положением по контролю за изменениями, сводиться по принципу «сверху-вниз», иметь постоянных жизненный цикл и несколько центров подотчетности, учитывать IRM-политику и профиль угроз, нетехнические аспекты и требования бизнес-логики. В основе должна лежать прозрачная схема пересмотра и актуальные современные технологии по работе с большими данными.

DEVELOPMENT OF COMMERCIAL ENTERPRISE SECURITY PROGRAM

U.A. ULASENKA, S.L. PRISCHEPA

Abstract

With the continuous development of information technologies the question of effective information security management is becoming increasingly important. This article describes step by step development of the security program that allows effectively manage information risk of the organization. The attention is drawn to the important organizational features that need to be considered when building safety documents for their quality implementation and update.

Список литературы

1. COSO Enterprise Risk Management – Integrated Framework [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.coso.org/guidance.htm. – Дата доступа: 5.03.2015.
2. Анализ подходов к верификации функций безопасности и мобильности [Электронный ресурс]. – Электронные данные. – Режим доступа: http://ipv6.ispras.ru/Verification_of_security.pdf. – Дата доступа: 5.03.2015.
3. Shon Harris: CISSP All-in-One Exam Guide // McGraw-Hill.
4. Dhillon G. // Information Systems Journal. 2006. Vol. 16, № 3. P. 293–314
5. COBIT 5 [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.isaca.org/COBIT/Pages/COBIT-5-russian.aspx. – Дата доступа: 5.03.2015.