УДК 65.012.8

ПРОЕКТНО-ОРИЕНТИРОВАННОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

А.С. Сафронов
Кандидат технических наук, доцент
Кафедра информационной безопасности
Институт радиотехники и телекоммуникаций
Одесский национальный политехнический университет
пр. Шевченко, 1, г. Одесса
Контактный тел.: 095-27-87-575
E-mail: AlexanderSafronov@rambler.ru, Alexx_s@ukr.net

Стаття присвячена аналізу проблем управління інформаційною безпекою організації. Розглянуто основні етапи створення системи інформаційної безпеки, виявлені особливості реалізації цих процесів у сучасних організаціях. Надані рекомендації з управління проектами в галузі інформаційної безпеки

Статья посвящена анализу проблем управления информационной безопасностью организации. Рассмотрены основные этапы создания системы информационной безопасности, выявлены особенности реализации данных процессов в современных организациях. Даны рекомендации по управлению проектами в области информационной безопасности

This article is dedicated to an enterprise information security management. Basic stages of information security system creation are examined and features of a modern implementation of these processes are considered. The recommendations on project management in information security are given

В настоящее время обеспечение информационной безопасности организации является проблемой актуальной и требующей адекватного понимания своей важности со стороны высшего руководства. Информационная безопасность организации — это состояние гарантированной защищённости ее информационной среды при обеспечении условий нормальной работы и развития организации.

Достижение необходимого уровня информационной безопасности (ИБ) организации — комплексная задача, требующая системного подхода, в общем случае, включает в себя следующие составляющие:

• Наличие соответствующей законодательной, нормативно-правовой и научной базы.

• Включение в структуру организации подразделений, обеспечивающих выполнение работ и контроль состояния ИБ организации.

• Наличие работников, обладающих необходимой компетенцией в вопросах защиты информации. Руководитель структурного подразделения, кроме знаний в области ИБ, должен также обладать компетенцией в управлении проектами и персоналом. В отдельных случаях допускается привлечения субподрядчиков для выполнения отдельных работ и даже проектов по ИБ, но полностью доверять обеспечение ИБ сторонней организации не рекомендуется.

• Доступность необходимых технических средств обеспечения ИБ.

Реализация ИБ состоит из двух этапов — ускоренное достижение минимально-необходимого уровня защиты информации в организации и постоянное обеспечение/совершенствование ИБ, обычно силами соответствующего подразделения организации. Причем первый этап носит ярко выраженные признаки проектной деятельности, т.к. создается уникальный результат для отдельно взятой организации при ограничениях по времени и средствам.

Как правило, на первом этапе проводится подробный анализ проблемы, определение условий и требований защиты информации, разрабатываются рекомендации по реализации, а также создается специальная структура, занимающаяся вопросами ИБ в организации.

Также на данном этапе формируется концепция и политики ИБ, положения, должностные инструкции и другая руководящая документация.

Особенностью создания системы ИБ в отечественных организациях является то, что кроме противодействия нелегальным угрозам ИБ, необходимо предпринять ряд мер по выполнению существующих норм и требований законодательства по ИБ, в частности к автоматизированной обработке конфиденциальной информации в компьютерных системах.

Причем затраты на эти меры могут превысить затраты на предотвращение нелегальных угроз.

Рис. 1. Начальный этап построения системы информационной безопасности

Второй этап — обеспечение/совершенствование уровня ИБ носит черты как операционной, так и проектной деятельности. Особенностью построения системы ИБ в отечественных организациях является то, что, как правило, они не готовы в полном объеме выполнить задачи первого этапа — в основном из-за ограниченности ресурсов, нехватки специалистов и недопонимания руководства. Поэтому все недоработки обычно переносятся на второй этап для постепенного выполнения силами созданного отдела ИБ. Также особенностью второго этапа является то, что при выполнении плановых мероприятий по ИБ часто еще до их завершения меняются условия, что требует новых мероприятий, часто переделывающих ранее полученные результаты. Таким образом получается эффект «бесконечного» проекта — из за различных причин увеличивается время проекта, а когда он завершается — его результаты уже не соответствуют изменившимся требованиям и условиям, и надо инициировать новый проект. Очевидно, что выполнение второго этапа ИБ разумно разбить на группу связанных микропроектов с правом руководителя отдела ИБ создавать, останавливать их и распределять ресурсы между ними соответственно глобальной стратегии обеспечения ИБ предприятия. В отличие от традиционного управления проектами, где главное внимание уделяется своевременности выполнения проекта не превышая запланированные затраты, здесь важнее эффективно создавать новые ценности для предприятия, выражающиеся в повышении уровня ИБ при минимизации рисков реализации угроз ИБ и часто связанных с ними рисков микропроектов.

В связи с тем, что на рассматриваемые проекты ключевое влияние имеют требования по ИБ организации и нестабильная среда окружения проектов, то интересным является применение японской методологии P2M, позволяющей в высокой степени учитывать стратегию компании при управлении отдельными и связанными проектами вместо традиционной методологии для управления данными проектами ИБ.

Литература

1. Ципес Г.Л., Товб А.С, Менеджмент проектов в практике современной компании. – М.: ЗАО «Олимп – Бизнес», 2006. – 304 с.
2. Сафронов А.С., Венедиктов Ю.И., Барабанов Н.А. Жизненный цикл системы управления информационной безопасностью организации – Тези доповідей V Міжнародної конференції «Управління проектами у розвитку суспільства» – К.:КНУБА, 2008. – с. 185–187.