

УДК 004.43(031)

## МЕТОДОЛОГИЯ УПРАВЛЕНИЯ ПРОЕКТАМИ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.М. Асташкин, аспирант МТУСИ; astapavv@gmail.com

**Ключевые слова:** информационная безопасность, защита информации, КСИБ, методология управления проектами.

Согласно Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации», информационная безопасность – это состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность (ИБ) автоматизированной информационной системы, в которой она реализована [1].

Из истории развития информационной безопасности. Понятие «информационная безопасность» возникло с появлением средств коммуникации и осознанием человеком наличия у отдельных людей и сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства коммуникации. По мере развития средств коммуникации усложнялись и совершенствовались методы и системы информационной безопасности. В истории развития ИБ можно выделить несколько этапов.

**Первый этап.** До появления технических средств коммуникации основными способами передачи информации на расстояние являлись почтовая связь и неэлектрическая (световая и звуковая) телеграфная связь. Главными недостатками последней были сравнительно небольшое расстояние передачи, зависимость от погодных условий и невозможность обеспечить скрытность передачи, поэтому предпочтение отдавалось почтовой связи.

Наиболее известным методом обеспечения ИБ почтовой связи было шифрование. Еще во времена Римской республики Гай Юлий Цезарь для секретной переписки со своими генералами использовал один из самых простых и наиболее распространенных методов шифрования – шифр сдвига, который впоследствии был назван в его честь: шифр Цезаря [2]. Основной задачей информационной безопасности в то время было сохранение в тайне сведений о событиях, фактах, месторасположении имущественных и военных ценностей, имеющих жизненно важное значение для человека лично или сообщества, к которому он принадлежал.

**Второй этап.** Появление технических средств коммуникации, и прежде всего электрической телеграфной связи, с одной стороны, помогло решить проблему скрытности, а с другой – резко увеличило количество передаваемой информации. В сложившейся ситуации для обеспечения безопасности передачи был использован опыт, накопленный на ранних стадиях развития ИБ, что привело к созданию более сложных шифров и систем шифрования. Первой из таких систем стала шифровальная машина «Энигма», используемая различными немецкими военными службами во время Второй мировой войны [2].

**Третий этап** развития ИБ начался с создания электронно-вычислительных машин (ЭВМ). Информационная безопасность обеспечивалась преимущественно ограничением физического доступа к ЭВМ. Но с момента объединения ЭВМ в локальную вычислительную сеть физических методов

ограничения доступа стало недостаточно, и вскоре к ним добавились способы ограничения доступа к входящим в состав сети устройствам хранения информации с помощью администрирования и управления доступом к сетевым ресурсам.

**Четвертый этап** – эпоха создания и развития глобальных информационно-коммуникационных систем. Для решения задач ИБ потребовалась разработка комплексных систем информационной безопасности (КСИБ), сочетающих в себе как технические, так и инженерные средства защиты.

**Управление проектами КСИБ.** Согласно данным научных исследований, с 1999 по 2006 г. количество информации возросло на 38% и достигло 161 экзбайт. А с 2006 г. этот показатель ежегодно увеличивается на 57% (см. рисунок).

С ростом количества информации становилось все труднее обеспечивать ее безопасность. В начале XXI века КСИБ уже представляли собой сложный набор подсистем и функций и охватывали все больше и больше областей. Возникла проблема управления проектами КСИБ.

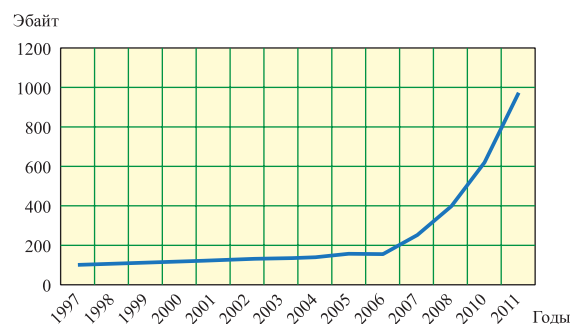
Следует заметить, что первые современные методы управления проектами появились в 50-е годы прошлого века. Тогда практически одновременно две проектные группы – Du Pont и Remington Rand – предложили методы управления сложными комплексами работ, получившие название Методика критического пути (Critical Path Method – СРМ). Независимо от них военно-морскими силами США была создана PERT (Program Evaluation And Review Technique) – методика для анализа и оценки длительности выполнения работ.

В настоящее время за рубежом насчитывается несколько институтов управления проектами, созданы многочисленные стандарты и методологии, такие как PMI, IPMA, PRINCE2 и т.д. Но все они имеют общий характер и не учитывают специфику системы информационной безопасности.

В России же сфера управления проектами только начинает развиваться, причем развитие в основном идет по пути заимствования зарубежных стандартов. Однако для успешного управления проектами КСИБ этого недостаточно. Необходимо не просто перенимать зарубежный опыт, но и адаптировать его к особенностям работы на территории нашей страны, учитывая специфику проектов систем ИБ.

Отсутствие стандартов и методологий управления проектами КСИБ приводит к появлению следующих проблем:

- реализация проектов не координируется;
- при оформлении проектов не используются общие нормы, условные обозначения и терминология;



- отсутствуют типовые технические решения, стандартные формы и образцы документов;
- четко не разграничены зоны ответственности участников проектной деятельности;
- принятие решений требует много времени;
- принимаются неоптимальные решения.

Рассмотрим подробнее некоторые из них. Нескоординированность деятельности подразделений компаний, отвечающих за различные подсистемы КСИБ (подсистема контроля и управления доступом, подсистема охранного телевидения и т.д.), приводит не только к простому подразделений в случае задержки сдачи подсистемы одним из них, но и к возникновению проблем функционирования подсистем как единого целого. Ошибка, допущенная на начальной стадии при проектировании одной из систем, влечет за собой переработку решений других.

Из-за отсутствия стандартизированной терминологии нет единообразия в оформлении документов. Нередко требуется их переработка и «подгонка» к единому стилю. Из-за отсутствия типовых технических решений КСИБ приходится каждый раз заново продумывать техническую составляющую системы, вместо того чтобы просто внести изменения в типовые решения, скорректировав их в соответствии с требованиями конкретного проекта.

Все эти факторы негативно сказываются на выполнении проектов КСИБ, влияя на качество и время их реализации, вызывая необходимость дополнительно привлекать к работе специалистов, что в итоге ведет к увеличению финансовых затрат.

**Структура и содержание методологии управления проектами КСИБ.** Снизить временные и финансовые затраты на реализацию проектов КСИБ могла бы разработка методологии управления проектами комплексной системы ИБ.

Методология, включающая в себя перечень правил и рекомендаций, направленных на решение задач по проектированию КСИБ, позволит:

- разграничить полномочия и ответственность участников проектной деятельности на разных этапах жизненного

цикла проекта;

- ввести единые правила исполнения проектов, обеспечив тем самым взаимопонимание и продуктивное взаимодействие всех участников проектной деятельности;
- осуществлять управленческий контроль за выполнением проекта на всех стадиях его жизненного цикла (от инициации до закрытия) благодаря использованию единой методологии и формализованного подхода к механизмам управления проектами;
- повысить качество решений, принимаемых специалистами, и ускорить их принятие;
- повысить эффективность контроля исполнения проектов со стороны руководителей;
- облегчить процесс обучения специалистов методам управления проектами.

Методология управления проектами КСИБ включает в себя множество инструментов, позволяющих повысить качество реализации проектов и снизить временные и финансовые затраты на их реализацию. В их числе: модели процессов жизненного цикла проектов КСИБ; типовые решения разработки КСИБ; система качества, позволяющая с помощью удобных методов и моделей отслеживать и оценивать качество реализуемого проекта; нормы, стандарты и правила выпуска стилистически грамотных однотипных документов и др.

**В целом разработка методологии предоставит удобный и практичный механизм эффективного управления проектами комплексной системы информационной безопасности, вобравший в себя опыт лучших мировых практик и учитывающий все нюансы данной сферы деятельности.**

#### ЛИТЕРАТУРА

1. Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации».
2. Черчхаус Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. — М.: Весь мир, 2007.

Получено 08.04.11