угроз информационной безопасности для реализации функций подавления источников угроз, анализа последствий вредоносных воздействий и восстановления корректности информационных процессов;

• оценка эффективности противодействия угрозам информационной безопасности.

В. Н. Чашкин
Государственная корпорация «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)»

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КАК ЭЛЕМЕНТ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ДЕЯТЕЛЬНОСТЬЮ ОРГАНИЗАЦИИ

Предлагается подход к формализации предметной области управления информационной безопасностью на основе процессной модели системы управления информационно-технологической (ИТ) деятельностью организации.

Информационно-технологическая деятельность рассматривается как деятельность, направленная на использование возможностей информационных технологий для результативного и эффективного достижения целей организации с учетом рисков, связанных с применением указанных технологий.

В качестве концептуальной платформы для построения управления ИТ-деятельностью предлагается использовать методологию **управления ИТ-услугами** — Information Technology Service Management (далее — методология ITSM), в основе которой лежит понятие ИТ-услуги, а ИТ-деятельность рассматривается как деятельность по предоставлению и поддержке ИТ-услуг, соответствующих текущим и будущим потребностям организации.

Основными характеристиками ИТ-услуги признаются: функциональность, доступность, мощность, безопасность, непрерывность, стоимость, требования к которым определяются целями бизнес-процессов организации.

Характеристики ИТ-услуг должны обеспечивать необходимые и достаточные условия реализации бизнес-процессов результативным и эффективным способом, повышая возможности бизнеса и устанавливая согласованную связь между целями организации и целями ИТ-деятельности. Принимаемые организацией решения о требованиях к характеристикам ИТ-услуги должны обеспечить баланс между качеством, стоимостью ИТ-услуги, бизнес-эффектом ее использования и сопутствующими ИТ-рисками.

В рамках методологии ITSM, используя в качестве базовых процессные модели управления, предлагаемые государственными стандартами менеджмента качества серии ГОСТ Р ИСО 9000 и библиотекой лучшего мирового опыта ITIL (Information Technology Infrastructure Library), определяется система в составе 15 процессов управления ИТ-деятельностью.

Система управления ориентирована на цели организации и включает в себя:

- процессы жизненного цикла ИТ-услуг;
- процессы контроля и подготовки решений, обеспечивающие качество и эффективность ИТ-услуг «по способу производства» путем совершенствования процессов жизненного цикла;
- процесс управления изменениями, обеспечивающий результативность и эффективность принимаемых решений, а также снижение риска негативных последствий планируемых изменений ИТ-услуг и процессов;

- процесс управления конфигурациями, регулирующий среду информационного взаимодействия процессов системы управления.

Одним из элементов системы является процесс управления безопасностью, цель которого — обеспечение в соответствии с потребностями организации необходимого уровня информационной безопасности ИТ-услуги как одной из ее характеристик. Указанной цели процесс управления безопасностью как один из процессов контроля и подготовки решений достигает путем установки правил работы процессов жизненного цикла, контроля их исполнения и достигнутого уровня информационной безопасности ИТ-услуг.

Предлагаемый подход позволяет:

связать управление информационной безопасностью с целями организации и конкретизировать задачи процесса в рамках системы управления на основе классификации угроз и рисков ИТ-деятельности [1, 3];

обеспечить комплексный подход к защите информации на жизненном цикле ИТ-услуг [1, 2, 5];

разработать унифицированную процессную модель системы управления информационной безопасностью организации [2, 3, 4];

создать системную основу:

- гармонизации стандартов в области информационных технологий, включая вопросы управления информационной безопасностью и ИТ-рисками в целом [3];
- разработки программ подготовки специалистов по комплексному обеспечению информационной безопасности автоматизированных систем [1, 5].

СПИСОК ЛИТЕРАТУРЫ:

1. *Завгородний В. И.* Особенности подготовки специалистов и менеджеров к управлению информационными рисками // Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов XV Всероссийской научной конференции. М.: МИФИ, 2008. С. 60–61.

2. *Круглов А. М., Поликуров О. В.* Управление информационной безопасностью в органах государственной власти // Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов XV Всероссийской научной конференции. М.: МИФИ, 2008. С. 81–82.

3. *Петров В. А., Петрова Т. В.* Стандартизация информационных технологий как средство повышения качества управления информационной безопасностью // Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов XV Всероссийской научной конференции. М.: МИФИ, 2008. С. 108–109.

4. *Плешков А. К.* Построение модели СМИБ кредитно-финансовой организации РФ // Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов XV Всероссийской научной конференции. М.: МИФИ, 2008. С. 111–112.

5. *Хорев П. Б.* Обучение методам и средствам защиты информации при подготовке в области информационных технологий // Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов XV Всероссийской научной конференции. М.: МИФИ, 2008. С. 142–143.