К наиболее важным внутренним источникам угроз относятся:

• использование телекоммуникационных информационных технологий, реализуемых преимущественно на аппаратно-программных средствах зарубежного производства;

• увеличение объемов хранимой и передаваемой информации, а также территориальная распределенность телекоммуникационных информационных сетей;

• недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

• недостаточная координация деятельности органов власти и управления, организаций, находящихся в пределах Брянской области, по формированию и реализации единой государственной политики в области обеспечения информационной безопасности;

• недостаточное финансирование мероприятий по защите информации в органах власти и управления, организациях, находящихся в Брянской области;

• недостаточное количество квалифицированных кадров в области защиты информации.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать государственные ресурсы, наличие множества преднамеренных и случайных угроз информационным ресурсам вызывают необходимость создания комплексных систем информационной безопасности и защиты информации органов государственного и муниципального управления субъектов Российской Федерации.

Разработка проекта создания комплексной системы информационной безопасности и защиты информации в органах государственного и муниципального управления Брянской области выполняется в два этапа.

На первом этапе определен перечень органов государственной власти и местного самоуправления Брянской области, разработан алгоритм проведения аудита информационной безопасности, сформирована анкета для оценки уровня информационной безопасности на оцениваемых объектах, разработаны базы данных, содержащие типовые рекомендации по обеспечению защиты информации, выполнено обследование органов исполнительной власти и местного самоуправления Брянской области и проанализированы результаты данного обследования.

На втором этапе на основе результатов аудита информационной безопасности разработан проект создания комплексной системы информационной безопасности в органах государственного и муниципального управления Брянской области, содержащий основные направления и план программных мероприятий по обеспечению защиты информации. Помимо этого, результатом второго этапа является экономическая оценка предлагаемых проектных решений.

В. Н. Финько
Главное управление внутренних дел по Краснодарскому краю

ПРОБЛЕМА ОПТИМИЗАЦИИ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Формулируются содержательная и формализованная постановка проблемы оптимизации информационной деятельности территориальных органов внутренних дел (ОВД) в условиях противодействия угрозам информационной безопасности. Приводятся пути ее решения.

В содержательном плане проблема оптимизации информационной деятельности территориальных органов внутренних дел в условиях противодействия угрозам информационной безопасности формулируется следующим образом.

Применительно к типовым условиям информационной деятельности территориального органа внутренних дел, заданному описанию его функционально-предметной структуры и характеристикам вредоносных воздействий, обусловленных угрозами информационной безопасности, необходимо разработать методы оптимального распределения информационных ресурсов органа в интересах обеспечения одновременной реализации трех процессов: информационного, процесса идентификации вредоносных воздействий, обусловленных угрозами информационной безопасности, и процесса устранения их последствий, обеспечивающих повышение эффективности информационной деятельности органа в условиях противодействия угрозам информационной безопасности.

Формально эту проблему можно сформулировать как совокупность задач выявления функционального резерва $\vec{R}^{(u)}$ информационной деятельности органа внутренних дел в интересах идентификации вредоносных воздействий, его распределения между процедурами информационного процесса и реализации в виде соответствующих средств с целью максимизации значения показателя $D(\omega_g^{(u)})$ его защищенности на множестве

$\Omega^{(u)} = \{ \omega_g^{(u)}(\vec{R}^{(u)}) \mid \omega_g^{(u)}(\vec{R}^{(u)}) \in \Omega^{(u)}, \mathrm{g} = 1, 2, \ldots, |\Omega^{(u)}| \}$

вариантов функционального резервирования и распределения функционального резерва в интересах устранения последствий угроз информационной безопасности с целью максимизации значения показателя $D(\omega_h^{(y)})$ защищенности информационного процесса на множестве

$\Omega^{(y)} = \{ \omega_h^{(y)}(\vec{R}^{(y)}) \mid \omega_h^{(y)}(\vec{R}^{(y)}) \in \Omega^{(y)}, \mathrm{h} = 1, 2, \ldots, |\Omega^{(y)}| \}$

вариантов функционального резервирования в интересах устранения последствий угроз информационной безопасности.

Формально это можно записать в виде:

$D(G(U(t)), V(t), \omega_g^{(u)}(\vec{R}^{(u)})) \to \max, \omega_g^{(u)}(\vec{R}^{(u)}) \in \Omega^{(u)}, \mathrm{g} = 1, 2, \ldots, |\Omega^{(u)}|$

и

$D(G(U(t)), V(t), \omega_h^{(y)}(\vec{R}^{(y)})) \to \max, \omega_h^{(y)}(\vec{R}^{(y)}) \in \Omega^{(y)}, \mathrm{h} = 1, 2, \ldots, |\Omega^{(y)}|,$

где $U(t)$ — параметр условий информационной деятельности;

$G(U(t))$ — функциональная структура этой деятельности;

$V(t)$ — характеристики вредоносных воздействий.

Оптимальный вариант $\omega_{(opt)}^{(u)}$ функционального резервирования информационной деятельности органа внутренних дел в интересах идентификации вредоносных воздействий определяется в соответствии с выражением:

$\omega_{(opt)}^{(u)} = \mathrm{argmax}\, D(\omega_g^{(u)}(\vec{R}^{(u)})),$

$\omega_g^{(u)}(\vec{R}^{(u)}) \in \Omega^{(u)},$

а оптимальный вариант $\omega_{(opt)}^{(y)}$ функционального резервирования в интересах устранения последствий угроз информационной безопасности — в соответствии с выражением:

$\omega_{(opt)}^{(y)} = \mathrm{argmax}\, D(\omega_h^{(y)}(\vec{R}^{(y)})),$

$\omega_h^{(y)}(\vec{R}^{(y)}) \in \Omega^{(y)}.$

Сформулированная проблема может быть решена путем представления в виде ряда задач, к числу которых относятся:

• определение оптимального объема функционального резерва информационной деятельности органа внутренних дел в интересах идентификации вредоносных воздействий;

• оптимальное распределение этого резерва между процедурами информационного процесса с целью создания ресурсов для реализации процесса идентификации вредоносных воздействий;

• реализация резерва в виде средств обнаружения и идентификации вредоносных воздействий;

• обоснование требований к объему функционального резерва в интересах устранения последствий

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;