Особое место в деятельности организаций занимает стратегическое планирование, представляющее собой комплекс решений и действий по разработке стратегий, необходимых для достижения целей организации, предприятия. «Стратегия представляет собой детальный всесторонний комплексный план, предназначенный для того, чтобы обеспечить осуществление миссии организации и достижение ее целей» (Басовский, Л.Е. Прогнозирование и планирование в условиях рынка. – М., 2011).

«Стратегия развития организации определяется в результате изучения внешнего окружения и возможных внутренних перспектив ее деятельности с учетом непредвиденных рыночных обстоятельств» (Бухалков, М.И. Планирование на предприятии. – М., 2011). Выработка стратегии торговой организации в настоящее время базируется на методологических принципах новой концепции управления, а именно «стратегического управления», которое давно уже активно внедряется в странах Западной Европы. Известно, что любое управление является нечетким и оно было основной областью применения нечеткой логики. Вызывает оптимизм тот факт, что в исходную идею о нечеткой логике укладываются представления об управлении. Так как задачи управления возникают почти во всех технологических процессах, как в обществе, так и на производстве, можно сделать непреложный вывод о том, что потребности в теории и возможности приложений нечеткой логики достаточно велики.

***К.С. Сорокина***
Научный руководитель ***В.В. Кузьминов***
*Филиал БГЭУ (Бобруйск)*

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ СО СТАНДАРТОМ COBIT

Проблема обеспечения внутренней информационной безопасности становится все более актуальной. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень.

С учетом данных тенденций в мировом сообществе отчетливо проявляется стремление к унификации требований к управлению ИТ и их безопасности. Наиболее ярким примером является разработка стандарта COBIT, который стал синтезом наиболее распространенных международных стандартов в области управления ИТ, аудита, контроля и информационной безопасности .

Система контроля COBIT отвечает потребностям рынка, поскольку:

- связана с требованиями бизнеса;
- организует виды ИТ-деятельности в виде понятной процессной модели;
- определяет основные ресурсы ИТ, на которые должны осуществляться воздействие;
- определяет цели контроля.

Бизнес-ориентация COBIT состоит во взаимосвязи целей бизнеса и ИТ, выявлении показателей и моделей зрелости для оценки достижений, определении соответствующих видов ответственности владельцев бизнеса и ИТ-процессов.

В соответствии со стандартом COBIT оценка и управление ИТ-рисками достигается с помощью:

- полного включения управления рисками в процессы управления как внутри, так и во вне, и его постоянного применения;
- проведения оценок рисков;
- выработки предложений и информирования о планах противодействия существующим рискам.

Результаты оцениваются с помощью следующих показателей:

- доля критичных целей ИТ, охваченных оценкой рисков;
- доля выявленных критичных ИТ-рисков, в отношении которых разработаны планы действий;
- доля планов по управлению рисками, утвержденных и принятых к исполнению.

До принятия решения о внедрении той или иной методологии управления ИТ-рисками следует убедиться, что она достаточно полно учитывает бизнес-потребности компании, ее масштабы, а также соответствует лучшим мировым практикам и имеет достаточно подробное описание процессов и требуемых действий.

Построение системы управления ИТ-рисками является более сложной задачей, нежели выбор методологии, и требует не только хороших теоретических знаний, но и практического опыта внедрения. Следует заранее предпринять действия, чтобы не допустить типичных ошибок, которые состоят в отсутствии доверия к полученным результатам оценки ИТ-рисков со стороны руководства, недостаточной обоснованности расходов на снижение ИТ-рисков, а также в сопротивлении внедрению мер снижения ИТ-рисков в бизнес-подразделениях и технических службах.

На практике заказчик всегда хочет получить не только результаты первоначальной оценки ИТ-рисков и рекомендации по их снижению, но и простой в использовании инструмент такой оценки.

Построение модели методологии управления ИТ-рисками на предприятии начинается с построения модели нарушителя. Модель нарушителя представляет собой некое описание типов злоумышленников, которые намеренно или случайно, действием или бездействием способны нанести ущерб информационной системе. Для управления рисками требуется идентифицировать возможные опасности, угрожающие обследуемой информационной системе. Таковыми могут являться, например, наводнение, отключение электропитания или атаки злоумышленников с последствиями разной степени тяжести. После проведения первичной оценки рисков, полученные значения следует систематизировать по степени важности для выявления низких, средних и высоких рисков. Методика управления рисками подразумевает несколько способов действий. Риск может быть принят, снижен, передан.