АНАТОМИЯ БЕЗОПАСНОСТИ

Рано или поздно руководитель производственного или торгового предприятия задумывается о том, как ему обезопасить свой бизнес и минимизировать потери. Конечно, о цунами или землетрясении сибирякам пока можно не задумываться, но как защитить себя от иных угроз? А вариантов может быть множество:
с территории предприятия похитили большую партию продукции, в магазине при инвентаризации не нашли плазменный телевизор, обиженный системный администратор уничтожил или передал конкурентам базу предприятия, или в конце концов, просто все сгорело после корпоративной вечеринки.
Может показаться, что подобные угрозы для бизнеса непредсказуемы и носят случайный характер. Но грамотный руководитель должен понимать: опасности цивилизации можно предугадать и заранее подготовиться к ним. Одним словом, безопасность вашего предприятия находится в ваших руках (почти по Семашко).

С начала 90-х годов вместе с предпринимательством развивались и прикладные науки безопасности бизнеса - науки выживания в условиях политических и экономических реформ. Одна из таких наук - Управление Предпринимательскими Рисками (УПР)
определяет комплекс мероприятий, направленных на прогнозирование и заблаговременное выявление негативных воздействий на ведение бизнеса и реализацию мер по их нейтрализации. Это довольно обширная тема, касающаяся всех аспектов безопасности ведения бизнеса. Мы затронем лишь верхушку «айсберга» безопасности - практические приложения.

Одно из них - Концепция безопасности предприятия. Это система взглядов на обеспечение безопасности от внешних и внутренних угроз во всех сферах жизнедеятельности предприятия. В Концепции формулируются важнейшие (стратегические) направления политики в области Управления Предпринимательскими Рисками.

В ходе подготовки проекта Концепции безопасности производится ряд специальных экспертиз деятельности предприятия. Одна из них - организационно-психологическая, которая дает оценку внешних факторов (информационных, экономических, юридических, физических), влияющих на успешность деятельности предприятия. Кадровая экспертиза позволяет оценить вероятность совершения персоналом противоправных действий.

Производится организационное проектирование, формируются предложения по оптимизации структуры предприятия, направленные на повышение эффективности деятельности структурных подразделений (в которые также включены вопросы управления предприятием и подбора кадров).

Проводится экспертиза деятельности службы безопасности предприятия, организационных и технических мер, предпринимаемых для защиты деятельности предприятия, ценностей, людских ресурсов на момент экспертизы.

Экспертиза включает в себя:

- полное организационное и техническое обследование промышленных и административных объектов предприятия для выработки предложений по эффективной и оптимальной (необходимой и достаточной) системе безопасности;
- оцениваются угрозы ведению бизнеса - как источники, так и способы зашиты с учетом трех компонентов: человека (модель нарушителя), природы, техногенной среды.

Технические средства безопасности вторичны, поэтому только после проведения организационно - психологических и кадровых экспертиз готовятся предложения по инженерным и техническим средствам безопасности. В зависимости от важности защищаемого объекта и объема финансирования,

они могут внедряться поэтапно либо в ограниченном объеме.

Существуют основные системы, без которых невозможно эффективно защитить свой бизнес. Это:

- система пожарной сигнализации и оповещения о пожаре;
- система пожаротушения (если необходима по нормам);
- инженерные средства охраны (техническая укрепленность);
- система охранной сигнализации;
- система тревожной сигнализации.

И дополнительные системы:

- телевизионная система охраны и наблюдения;
- система контроля и управления доступом.

Важными этапами построения системы безопасности на объекте являются:

- разработка и согласование с заинтересованными службами тактики охраны с учетом категории объекта, анализа угроз и модели нарушителя;
- полная инвентаризация существующих технических средств охраны объекта и организационных мероприятий;
- подготовка рекомендаций по проведению организационно-технических мероприятий, необходимых для приведения охраны объекта в соответствие с моделью;
- подготовка и согласование с заказчиком технического задания (ТЗ) и проектно-сметной документации на систему безопасности объекта.

При подготовке ТЗ и проекта используются действующие государственные и ведомственные нормативные документы, предложения и замечания заинтересованных лиц заказчика, охранного предприятия или ведомственных и государственных структур надзора. Важными этапами реализации проекта является технический надзор за проведением работ и сдача системы безопасности объекта в эксплуатацию. Современные системы безопасности достаточно сложны, поэтому по окончании всех работ, как правило, требуется дальнейшее техническое и организационное сопровождение системы безопасности и ее подсистем на объекте.

Сопровождение системы включает в себя:

- технический надзор за правильной эксплуатацией, разработка инструкций по эксплуатации и их внедрение;
- заключение с фирмой-подрядчиком договоров на техническое обслуживание существующих систем безопасности, подготовленными и сертифицированными специалистами;
- проведение плановых регламентных работ в полном объеме;
- сопровождение гарантийного и послегарантийного ремонта с заменой неисправного оборудования на время ремонта из резервного фонда;
- работа с администраторами безопасности;
- работа с базами данных и конфигураторами систем, внедрение изменений в программное обеспечение;
- зашита аппаратно-программных средств от несанкционированного доступа.

Важным элементом сопровождения системы на объекте являются организационные и инженерно-технические мероприятия по защите информации:

- доступ к информации о состоянии системы к аппаратным средствам, протоколам событий, базам данных должен осуществляться в соответствии с категориями доступа к информации, должностными инструкциями и установленному регламенту;
- инженерная и техническая зашита помещений, в которых располагаются рабочие места и оборудование;

- инженерная и техническая защита систем коммуникаций;
- ключевая зашита рабочих мест;
- криптографическая зашита информации, поступающей с удаленных объектов.

Нельзя забывать об энергоснабжении системы безопасности. Ее работоспособность должна поддерживаться надежной и защищенной системой бесперебойного электропитания с возможностью резервирования.

При подготовке статьи использовалась методическая литература по УПР и выдержки из проекта «Концепции безопасности» одного из крупных производственных предприятий Западной Сибири, в подготовке которого участвовало ООО НПП "Лем".

Трапезников Станислав