Проблемы качества требований безопасности и возможные пути их решения

А. А. Кононов, Д. А. Никитин,
А. К. Поликарпов, А. В. Сичкарук

Как известно, одной из основных причин техногенных чрезвычайных происшествий (ЧП), катастроф, событий нарушения безопасности является человеческий фактор (ЧФ), и даже там, где в качестве причины указывается фактор технический, природный или какой-либо иной, все равно глубокий анализ произошедших событий позволяет выявить в качестве одной из основных причин нанесенного ущерба и его масштаба именно ЧФ.

Но если разобраться с тем, что стоит за этим понятием — «человеческий фактор», то это, как правило, безответственность, или недостаточная ответственность исполнителей тех или иных работ или функций.

В то же время, было бы неправильно обвинять в безответственности только исполнителей. Потому что их ответственность является в немалой степени качеством формируемым и управляемым.

Таким образом, еще более глубокой причиной невозможности обеспечить безопасное функционирование объекта, на котором происходит ЧП, является неспособность или принципиальная невозможность в сложившихся условиях обеспечить руководством ответственность подчиненных.

В то же время, было бы совершенно неправильно сказать, что в управлении вообще и в управлении рисками и безопасностью в частности, там, где происходили ЧП фактор ответственности исполнителей игнорировался. Правильно было бы отметить, что на сегодняшний день в отдельных структурах нет достаточного понимания влияния на него ряда других факторов, что в свою очередь влечет за собой пренебрежение этими факторами и, как следствие, их неконтролируемое деструктивное влияние.

Всемирно известен феномен так называемых «итальянских» забастовок. Его смысл заключается в том, что в тех областях деятельности, в которых забастовки законодательно запрещены, итальянцы первыми научились показывать свое недовольство условиями труда и его оплаты. Они просто с педантичной строгостью начинали выполнять все требования всех инструкций и положений, регламентирующих их работу. И вся деятельность организаций, в которых они работали, останавливалась. Настолько противоречивой и парализующей оказывалась система предъявлявшихся к их деятельности требований. О том, что подобные проблемы свойственны не только Италии, можно судить по тому, что подобного вида забастовки распространены и в других странах (в англоязычных странах для них используется термин «work-to-rule»).

И это, конечно же, не все. Вполне естественно полагать, что наиболее важные требования определяются законодательством. Относительно законодательств некоторых стран иногда говорят, что строгость законов в них компенсируется отсутствием контроля их исполнения. Можно встретить мнение, что именно последнее нередко спасает реальные сектора экономики от полной остановки и разорения.

Среди основных объективных причин такого положения вещей можно назвать следующие:

- быстрое изменение обстоятельств и условий осуществления регламентируемой деятельности;
- недостаточно полный учет возможного негативного влияния вновь вводимых требований на осуществление регламентируемой деятельности;
- недостаточно полный анализ существующей системы требований, и влияния вновь вводимых требований на непротиворечивость, и избыточность результирующей системы требований;
- принципиальная невозможность предвидения всех последствий введения новых требований;
- слишком большие и сложные организационные структуры.

Таким образом, можно констатировать наличие серьезных проблем качества систем требований. Особое негативное влияние такого рода проблемы могут иметь, если они касаются вопросов безопасности. Если система требований такова, что часть ее требований противоречива, избыточна, неисполнима в конкретных условиях, то это может стать источником культивирования безответственного отношения к проблемам безопасности в целом.

Среди возможных путей решения такого рода проблем можно назвать следующие:

- моделирование и исследование систем требований, регламентирующих отдельные сферы деятельности, особенно при внесении в них изменений и при существенных изменениях в тех областях деятельности, которые они регламентируют, или изменении во внешнем окружении этих областей;
- регулярный всеобъемлющий контроль выполнения всей системы требований каждым из субъектов, к которым относится хоть какая-то часть из этих требований, с анализом причин каждого случая невыполнения или неполного выполнения требований, с анализом реакции исполнителей и учетом их оценки качества требований, с доработкой систем требований на основе полученной информации;
- внезапный выборочный контроль (мониторинг) выполнения требований с анализом причин каждого случая невыполнения или неполного выполнения требований и доработкой систем требований, если невыполнение требований вызвано несовершенством системы требований;
- разделение требований на те, выполнение которых безусловно обязательно, и на те, выполнение которых является рекомендуемой практикой, но невыполнение которых допустимо, если следование им в конкретных условиях непосильно экономически, будет наносить ущерб конкурентоспособности или невозможно по каким-либо иными причинам.

В качестве положительного опыта решения проблем качества требований в сверхсложной, имеющей национальный масштаб организационной системе с десятками тысяч подразделений самого разного уровня, в которых выполняются критические процессы и операции с большим количеством требований к безопасности каждой из них, может быть приведен опыт Банка России в области обеспечения безопасности электронных платежных технологий [1].

Пять лет назад в Центральном банке Российской Федерации был внедрен разработанный в Институте системного анализа Российской академии наук распределенный программный комплекс «АванГард», который позволил объединить, затем распределить по исполнителям и довести до каждого работника требования к безопасности, содержащиеся в десятках документов, регламентирующих безопасность банковских операций. Далее был установлен режим ежеквартальной отчетности о выполнении требований на основе самооценки безопасности подраз-

делений, осуществляемый руководством региональных расчетных систем. В то же время, Главное управление безопасности и защиты информации Банка России периодически осуществляет инспекционные контрольные проверки безопасности региональных расчетных систем, позволяющие судить о корректности отчетности выполнения требований. Исполнители стали очень критично относиться к тем требованиям, выполнение которых имело какие-либо проблемы. В результате образовавшейся обратной связи от исполнителей поступали оценки качества требований, и система требований дорабатывалась.

Наработанный позитивный опыт позволил главному инициатору и идеологу разработки и внедрения системы «АванГард» в Центральном банке РФ, заместителю начальника Главного управления безопасности и защиты информации Банка России А. П. Курило создать рабочую группу по разработке нормативной базы обеспечения информационной безопасности организаций всей банковской системы Российской Федерации. В результате работы этой группы был создан комплект документов [2–6], который создает прочную нормативную базу реального контроля состояния безопасности национальной банковской системы на основе качественной системы требований к безопасности и периодической самооценки по этим требованиям безопасности информационных систем каждого банка, каждой кредитной организации страны.

Этот опыт и разработанные документы могли бы послужить в качестве хорошего подспорья в решении проблем управления рисками и безопасностью и в других областях и отраслях деятельности, где есть критически важные объекты и процессы.

Литература

1. *Владимирова Т. Н.* Опыт работы по внедрению системы мониторинга информационной безопасности платежной системы Банка России // Информационный бюллетень Главного управления безопасности и защиты информации Центрального банка Российской Федерации. 2005. № 1. С. 47–56.
2. Стандарт Банка России СТО БР ИББС-1.0-2006. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Принят и введен в действие Распоряжением Банка России 26 января 2006 г. № Р–27. М.: Банк России, 2006.
3. Стандарт Банка России СТО БР ИББС-1.1-2007. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». Принят и введен в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–345. М.: Банк России, 2007.

4. Стандарт Банка России СТО БР ИББС–1.2–2007. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС–1.0». Принят и введен в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–346. М.: Банк России, 2007.
5. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС–1.0» Приняты и введены в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–347. М.: Банк России, 2007.
6. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС–1.0». Приняты и введены в действие Распоряжением Банка России от 28 апреля 2007 г. № Р–348. М.: Банк России, 2007.