МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Сучасні технології у промисловому виробництві

М А Т Е Р І А Л И

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ ВИКЛАДАЧІВ, СПІВРОБІТНИКІВ, АСПІРАНТІВ І СТУДЕНТІВ ФАКУЛЬТЕТУ ТЕХНІЧНИХ СИСТЕМ ТА ЕНЕРГОЕФЕКТИВНИХ ТЕХНОЛОГІЙ
(Суми, 14–17 квітня 2015 року)

ЧАСТИНА 1

Конференція присвячена Дню науки в Україні

Суми
Сумський державний університет
2015

ОСОБЕННОСТЬ ИСПОЛЬЗОВАНИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ISO 31000 И ISO 27005 В СФЕРЕ УПРАВЛЕНИЯ РИСКАМИ

Янченко В. Н., аспірант; Опрыско О. Б., магістрант;
Ивченко А. В., доцент

Любое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения одних социальных проблем и открывая широкие перспективы для развития личности и общества, всегда вызывает обострение старых или порождает новые, ранее неизвестные проблемы, становится источником новых потенциальных опасностей.

Без должного внимания к вопросам обеспечения безопасности, последствия перехода общества к новым технологиям могут быть катастрофическими для него и его граждан.

Применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям с целью доступа к критичной информации и дезорганизации работы автоматизированных систем.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

- обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;
- расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи;
- повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;
- вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;
- концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;
- количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
- отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем;

 многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации;

 ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации;

 увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов);

 развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Проанализировав все вышесказанное, приходим к выводу, что угрозы информационной безопасности являются реальными и последствия могут быть очень серьезными. Для того чтобы защитить информацию эффективно, необходимо иметь возможность выбирать наиболее подходящие меры безопасности. Это может быть достигнуто путем определения основных рисков информации в системе, а затем внедрения соответствующих мер защиты.

С этой целью были разработаны международные стандарты (МС) ISO 27001 и ISO 31000. В МС ISO 31000 показан общий процесс управления рисками для всех секторов. Стандарт содержит рекомендации о том, как организовать управление рисками в организациях – он не сосредоточен исключительно на рисках информационной безопасности; он может быть использован для различных типов рисков, включая непрерывность бизнеса, рынок, валюта, кредитных, операционных и других.

В свою очередь, МС ISO 27001 является стандартом, который описывает, как компания должна организовать свою информационную безопасность – она основана на принципах управления рисками, а это означает, что компания должна выбрать гарантии (контроля безопасности), только если есть неприемлемо риски, которые должны быть обработаны.

ISO 27001 является как большой процесс управления рисками для крытой области: информационной безопасности. Если же есть необходимость пойти глубже в управлении информационными рисками, можно использовать 27005.

И так, чтобы выполнить управление рисками в области информационной безопасности, необходимо адаптировать 31000. Это цель, роль и борьба ISO 27005.

Таким образом, оба рассмотреных стандарта не содержат методологии обеспечения безопасности, содержат лишь требовани (являются лишь описанием «что делать» для выполнения процесса управления рисками, в общей или в конкретной области информационной безопасности), но не объясняют «как реализовать» данные требования.