АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ СТАНДАРТА ISO/IEC 27001

Дуравкин Е.В., Гладий Л.В.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина,14, каф. Телекоммуникационных систем,
тел.(057) 702-55-92), E-mail: tcs@kture.kharkov.ua; факс: (057) 702-13-20

The information is one of the most important business resources who provides the organizations additional cost and thereof requires protection. ISO/IEC 27001 is the formal set of specifications against which organizations may seek independent certification of their Information Security Management System (ISMS). ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing an organization's information security risks. The standard covers all types of organizations such as commercial enterprises, government agencies and non-profit organizations.

На сегодняшний день информация является одним из наиболее ценных активов компаний. Следовательно, успешность бизнес процессов компании на прямую связанно с вопросами обеспечения безопасности информационных активов.

Правильная организация системы менеджмента информационной безопасности (СМИБ) позволяет минимизировать не только риски потерь информации, важной для компании, но и снижает общую стоимость владения системой безопасности. По статистике группы компьютерной безопасности по реагированию на инциденты (CERT) более 60% организаций регулярно терпят убытки, связанные с нарушением информационной безопасности и не способны оценить ущерб или хотя бы обнаружить многие из этих нарушений.

Отчет группы CERT за 2010 год показал, что киберпреступники начинают отказываются от традиционных методов массовой рассылки спама и переходят к персонализированным атакам. Главная цель этих атак – кража интеллектуальной собственности. Ежегодно такие атаки, организуемые с учетом особенностей того или иного объекта и содержащие вредоносные программные коды, нацеленные на конкретную группу пользователей и даже на отдельного пользователя, наносят ущерб в $1,29 млрд.

Успех целевых атак, как и других киберпреступлений, строится на технических уязвимостях и людской доверчивости.

Против таких атак труднее всего защищаться, тогда, как они могут нанести значительный ущерб. Одним из наиболее эффективных способов защиты от таких атак является построение единой системы информационной безопасности в компании, которая будет в себя включать и организационные и технические процедуры защиты информации.

Международный стандарт менеджмента информационной безопасности ISO/IEC 27001 предназначен для разработки системы управления информационной безопасностью организации [1].

Положения стандарта описывают такие аспекты:

- Политика безопасности;
- Организационные методы обеспечения информационной безопасности;
- Управление ресурсами;
- Пользователи информационной системы;
- Физическая безопасность;
- Управление коммуникациями и процессами;
- Контроль доступа;
- Приобретение, разработка и сопровождение информационных систем;
- Управление инцидентами информационной безопасности;
- Управление непрерывностью ведения бизнеса.

Внедрение СМИБ позволит:

- Выявить основные угрозы безопасности для существующих бизнес-процессов;

- Оценить риски информационной безопасности и принимать решения на основе бизнес-целей компании;
- Обеспечить эффективное управление системой в критичных ситуациях;
- Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности)
- Четко определить личную ответственность сотрудников компании за нарушения безопасности;
- Снизить стоимость владения системой безопасности компании;
- Продемонстрировать клиентам, партнерам свою приверженность к информационной безопасности;
- Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках;
- Подчеркнуть прозрачность и чистоту бизнеса перед законом.

Такая система менеджмента информационной безопасности, построенная в соответствии с требованиями стандарта ISO/IEC 27001, представляет собой гибкий инструмент, использование которого позволит выявить возможные угрозы информационной безопасности и уязвимости в системе защиты, разрабатывать и внедрять мероприятия организационного, технического, физического характера, нацеленные на снижение вероятностей возникновения таких угроз, а также проводить оценку эффективности подобных мероприятий.

Особенностью данного стандарта является то, что он касается не только вопросов управления в компьютерных сетях, но и вопросов разработки политики безопасности, работы с персоналом, обеспечения непрерывности процесса производства, а также юридических требований.

При построении СМИБ в соответствии с требованиями ISO/IEC 27001 за основу берется модель PDCA [2]:

- Plan (Планирование) — фаза создания системы управления информационной безопасностью, создание перечня активов, оценки рисков и выбора мер;
- Do (Действие) — этап реализации и внедрения соответствующих мер;
- Check (Проверка) — фаза оценки эффективности и производительности системы управления информационной безопасностью. Обычно выполняется внутренними аудиторами.
- Act (Улучшения) — выполнение превентивных и корректирующих действий

В связи с тем, что требования к данному стандарту имеют общий характер, его можно применять к широкому кругу организаций – малых, средних, больших – занимающихся деятельностью в различных областях, особенно в тех, где вопросы защиты информации особенно важны, например, в таких отраслях, как здравоохранение, работа с финансами, страхование, информационные технологии и госучреждения.

Данный стандарт хорошо согласовывается и с другими стандартами систем менеджмента информационной безопасности, таких как 9001:2000 и ISO 14001:2004, что связано с использованием общих принципов защиты информации.

Использование данного стандарта при организации СМИБ на предприятии позволит снизить и оптимизировать затраты на поддержку системы безопасности. Будут финансироваться только те направления безопасности, которые закроют самые опасные риски для определенного предприятия.

Литература:

1. ISO/IEC 27001 Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. – Взамен BS 7799-2:2002; Введ. 18.10.05. 2. Praveen Gubta, Beyond PDCA - A New Process Management Model // Quality Progress. – July 2006, Vol. 39, No. 7, – P. 45-52.