Литература

1. Экономический словарь//http://abc.informbureau.com/html/einaeaad.html
2. Верин В.П., Преступления в сфере экономики. - М., Дело.2002.
3. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия // Управління розвитком. – 2008. – № 6. – С.17-21.
4. Кавун С.В., Сорбат И.В. Инсайдер – угроза экономической безопасности // Управління розвитком. – 2008. – № 6. – С.7-11.
5. Олейников Е. А. Экономическая и национальная безопасность: Учебникдля вузов. – М.: Экзамен, 2005. – 768 с.
6. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк.– Х.: ХНЕУ, 2006. – 240 с.
7. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

ВНЕДРЕНИЕ СТАНДАРТА ISO 27001 В ОРГАНИЗАЦИИ

А. ХВОСТОВЕЦ,
FLT (Молдова)

This piece of information covers some major aspects regarding the ISO/IEC 27001 Standard, including its' brief description and implementation within organization.

Информация зачастую является ключевым активом компании, а ее защита - приоритетной задачей. Получение сертификации по стандарту ISO 27001 позволит сохранить и защитить Ваши информационные активы.

ISO 27001 является единственным пригодным для сертификации международным стандартом, определяющим требования к Системе Управления Информационной Безопасностью (СУИБ). Этот стандарт предназначен для обеспечения выбора адекватных и соразмерных средств защиты (контролей).

СУИБ помогает защитить Ваши информационные активы и придать уверенность любым заинтересованным сторонам, особенно Вашим клиентам. Стандарт определяет требования к созданию, внедрению, эксплуатации, контролю, обслуживанию и постоянной оптимизации СУИБ.

ISO 27001 – международный стандарт по информационной безопасности. Стандарт разработан Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссией (IEC). Данный стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы Управления Информационной Безопасностью (СУИБ).

ISO 27001 подходит для любой организации, крупной или малой, относящейся к любой отрасли и расположенной в любой части мира. Этот стандарт осо-

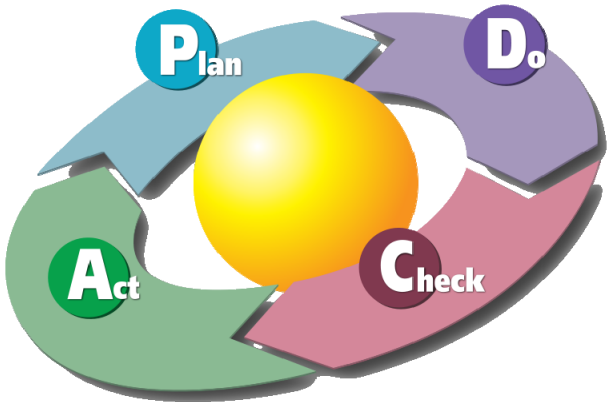
бенно полезен там, где защита информации приобретает очень важное значение, например в таких отраслях, как финансы, здравоохранение, госучреждения и IT.

ISO 27001 также эффективно используется в организациях, управляющих информацией по поручению другой стороны, например в компаниях, занимающихся аутсорсингом IT-ресурсов. Он может служить клиентам гарантией того, что их информация надежно защищена.

Ключевой характер в стандарте ISO 27001 носят **анализ рисков** и **оценка рисков**. Под анализом рисков *понимается систематическое использование информации для выявления источников и для оценки степени риска*. Под оценкой рисков - *целостный процесс анализа риска и оценки значительности риска.*

Организация может быть сертифицирована аккредитованными агентствами в соответствии с данным стандартом. Процесс сертификации состоит из трех стадий:

- **Стадия 1** - изучение аудитором ключевых документов Системы Менеджмента Информационной Безопасности — Положения о применимости (SoA), Плана Обработки Рисков (RTP), и др. Может выполняться как на территории организации, так и путём высылки этих документов внешнему аудитору.
- **Стадия 2** - детальный, глубокий аудит, включая тестирование внедренных мер и оценку их эффективности. Включает полное изучение документов, которые предусматривает стандарт.
- **Стадия 3** - выполнение инспекционного аудита для подтверждения, что сертифицированная организация соответствует заявленным требованиям. Выполняется на периодической основе.



Система управления информационной безопасностью (СУИБ) — часть общей системы менеджмента, основанная на подходе анализа бизнес-рисков и направленная на создание, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности (ISO 27001:2005).

В случае построения в соответствии с требованиями стандарта ISO 27001: 2005 основывается на модели Plan-Do-Check-Act:

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

Литература

1. Стандарт ISO2700:2005
2. Материалы сайта BSI (http://www.bsi.ru)
3. Материалы сайта ISO (http://www.iso.org)

СОТОВЫЕ СЕТИ ГСМ И ИХ БЕЗОПАСНОСТЬ

Михал СЭРВА,
Политехнический институт (Вроцлав, Польша)

В Польше первые системы сотовых сетей стали доступными в 1991 году (фирма Центртел). Это была самая простая аналоговая сотовая сеть первого поколения 1Г (*first-generation*), работающая на частоте 450MHz. Она покрывала свыше 90% территории страны. Системы сотовых сетей подвергнуты угрозам безопасности в такой же степени, как и проводные сети. Кроме того, в отношении радиотрансфера информации появляются дополнительные опасности.

Аналоговые системы (первого поколения) не были защищены, прежде всего, от радиоперехвата и использования для создания клона телефона. Такой обман был довольно распространенным в данном типе сотовых сетей и стал причиной больших финансовых потерь операторов. Эти системы была также неустойчивы к перебоям. У них не было международного роуминга, а также передача данных происходила очень медленно. Это вызвало появление цифровой системы второго поколения 2Г (2G), называемой системой ГСМ. Теоретическая скорость данных в такой системе достигала 9,6 кб/с, а трансмиссия речи с кодированием колебалась в пределе 13 кб/с. Были добавлены также узкополосные услуги такие как: данные, SMS, VMS, Fax. Система ГСМ900 была в Польше внедрена в 1996 году фирмами: Польская Телефония Цифровая (PTC ERA GSM) и Полкомтел (PLUS GSM). Следующей системой была система 2,5Г (2,5G), к которой добавлена трансмиссия данных GPRS. Система 2,5Г стала переходной к технологии третьего поколения в которой добавлена трансмиссия EDGE. Это сделало возможным трансмиссию с теоретической пропускной