УДК 658

# МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Сакович В.А., студ., Махонь А.Н., к.т.н., доц.**
*Витебский государственный технологический университет,*
*г. Витебск, Республика Беларусь*

Формирование системы менеджмента информационной безопасности (СМИБ), ее эксплуатация, контроль и постоянное улучшение – необходимое условие для создания конкурентоспособного предприятия. Внедрение СМИБ подразумевает разработку и реализацию процедур, направленных на систематическую идентификацию, анализ и снижение рисков информационной безопасности, то есть рисков, в результате которых информационные активы потеряют свойства конфиденциальности, целостности и доступности. Защита информационных активов за счет менеджмента информационной безопасности является существенной для способности организации достигать своих целей, а также поддержания соответствия законодательным требованиям и имиджа.

Серия стандартов ISO/IEC 27000 состоит из взаимосвязанных документов. В стандарте ISO/IEC 27001 описаны процессы СМИБ, в основе которого лежит цикл PDCA. Эти процессы должны охватывать все аспекты управления инфраструктурой организации, так как информационная безопасность – это результат устойчивого функционирования процессов, связанных с информационными технологиями.

При внедрении СМИБ каждая организация обязана подумать и о создании системы управления рисками. Риск информационной безопасности представляет собой потенциальную возможность использования уязвимостей информационного актива конкретной угрозой с причинением ущерба организации. Ущерб от реализации рисков информационной безопасности может быть как материальным (потеря дохода, выплаты судебным искам), так и нематериальным (снижение репутации и уровня доверия). Риск оценивается вероятностью причинения ущерба и величиной ущерба, наносимого организации в случае осуществления угрозы безопасности.

Во многих странах в приоритете информационная безопасность в сфере систем мобильной связи. Система обеспечения защиты информации в каждой конкретной системе мобильной связи, а также подход к ее построению и реализации индивидуальны. Однако во всех случаях для создания эффективной комплексной защиты информации в них необходимо:

1. Выявить все возможные факторы, влияющие на уязвимость информации, подлежащей защите, то есть построить модель угроз информационной безопасности и выявить каналы утечки.
2. Обосновать возможные методы защиты информации, направленные на устранение выявленных угроз.
3. Создать комплексную систему, обеспечивающую качественное решение задач защиты информации, основанную на минимизации ущерба от возможной утечки информации.

Методами обеспечения информационной безопасности в сфере мобильной связи являются: защита абонентов, защита передаваемых сообщений, шифрование сообщений, аутентификация и абонента, и сети.