КУРСОВА РАБОТА

НА ТЕМА:

КРИТЕРИИ ЗА ЕФЕКТИВНОСТ НА МЕТРИКИТЕ ЗА КИБЕРСИГУРНОСТ

Изготвил: **Проверил:**

София, 2017

УВОД

Изпълнението на мерки за оценка на ефективността на системата за управление на информационната сигурността (ISMS) е свързано с голямо количество работа за получаване на показатели за качество. Взаимодействието между дейностите на ISMS се осъществява чрез оценки. По време на оценката на атрибутите на обектите се проучва документацията, работните и технически тестове[1]. Работата с документацията и интервюирането несъмнено е важна част от проверките, но те имат някои недостатъци - ръчно събиране на информация, ниска степен на автоматизация, субективност на оценките, зависимост от нивото на компетентност на одитора[2]. Техническите тестове предоставят количествени оценки за качеството на ISMS. Одиторът действа като външен обект въведен изкуствено във функционирането на ISMS. Техническите методи за изпитване могат да се извършват с помощта на известни автоматизирани средства - софтуерен инструмент за оценка на състояние IS - CSET (Cyber Security Evaluation Tool), мрежов скенер XSpider, и т.н.. В резултат на това въз основа на получените показатели за качество, ръководството извършва анализ на дейността на ISMS и определя посоката на по-нататъшно развитие на системата. По време на анализ на ефективността в съответствие с изискванията на ръководните документи[3] се извършва оценка на показателите за качество на получените мерки и средства за контрол и управление. ISMS не отчита несигурността на измерените атрибути.

Разработката анализира какви могат да бъдат критериите за ефективност на метриките в т.ч. какво представляват "добрите" метрики и как те може да се използва за подобряване на ефективността на информационната сигурност. Целта е да се предостави концептуална база, необходима за по-доброто разбиране на киберсигурността.

1. Определение за "метрики"

Съществува известна двусмисленост по отношение на това кое е точното определение на термина „метрики за сигурност“ за защита на информацията. Обикновено термините (сигурност) метрика и мярка са склонни да се използват

[1] ISO/IEC 19011:2011. Guidelines for auditing management systems. 11.11.2011. Geneva, International Organization for Standardization. 44 p.

[2] Аксенов В.В. Аудит системы менеджмента информационной безопасности. Руководство [Электрон- ный ресурс]. Режим доступа: itsec.by/wp-content/uploads/2012/10/Auditors-Guide-ISO-27001-onRussian.pdf, свободный. Яз. рус. (дата обращения 20.04.2014)

[3] ISO/IEC 27000:2013. Information security management systems – Overview and vocabulary. 14.01.2013. Geneva, International Organization for Standardization. 25 p.