ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ғаниев Салим Каримович, Каримов Мажид Маликович, Ташев Комил Ахматович

АХБОРОТ ХАВФСИЗЛИГИ

(Ахборот-коммуникацион тизимлар хавфсизлиги)

Техника фанлари доктори, профессор С.С. Қосимов умумий таҳрири остида

Ўзбекистон Республикаси Олий ва ўрта махсус таълим вазирлиги томонидан техника олий ўқув юртлари бакалавриат босқичи талабалари учун ўқув қўлланма сифатида тавсия этилган

«ALOQACHI» – 2008

Ғаниев Салим Каримович, Каримов Мажид Маликович, Ташев Комил Ахматович. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма Т., «Aloqachi», 2008, 382 бет.

Ушбу қўлланма компьютер тармоқлари ва корпоратив ахборот тизимларини яратишда ва ишлатишда ахборотни ҳимоялашнинг долзарб муаммоларига бағишланган. Компьютер тармоқлари ва тизимларига таҳдид хиллари ҳамда локал ва корпоратив тармоқларни Internet-атакалардан ҳимоялаш усуллари ва воситалари муҳокама этилади. Электрон бизнес ва электрон тижоратда ахборот хавфсизлигини таъминлаш муаммосига алоҳида эътибор берилади. Ахборот хавфсизлиги концепцияси таърифланади ва тармоқларда хавфсизлик сиёсати аникланади.

Маълумотларни ҳимоялаш технологияси, тармоқ хавфсизлигининг базавий технологияси, суқилиб киришларни ва тармоқ хавфсизлигини бошқариш таҳлилланади. Хусусан, ахборотни замонавий криптографик ҳимоялаш воситаларининг принциплари, алгоритмлари ва протоколлари кўрилади; тармоқлараро экранларнинг турли хиллари тавсифланади ва уларни ишлатиш бўйича тавсиялар берилади; Internet хилидаги глобал очиқ тармоқларнинг очиқ коммуникациялари орқали криптоҳимояланган виртуал туннелларни шакллантириш усуллари ва воситалари муҳокама этилади; корхона ахборот ресурсларидан масофадан хавфсиз фойдаланишни таъминлаш масалалари кўрилади; маълумотларни узатиш тармоғида ахборотни ҳимоялаш масалалари ва уларни ечиш йўллари тавсифланади: симсиз тармоқ концепцияси, симсиз тармоқ хавфсизлигига таҳдидлар, симсиз тармоқ хавфсизлиги муаммоси баён этилади; тармоқ хавфсизлигини бошқариш усуллари ва воситалари таҳлилланади.

Хавф-хатарларни таҳлиллаш ва бошқариш асосида корхона ахборот хавфсизлиги тизимини қуриш методологияси таърифланади.

Қўлланма олий ўқув юртлари талабаларига, ахборот технологиялари, компьютер тизимлари соҳасида фаолият кўрсатувчиларга мўлжалланган.

***

Данное пособие посвящено актуальным проблемам защиты информации при создании и использовании компьютерных сетей и корпоративных информационных систем. Обсуждаются виды атак на компьютерные сети и системы, а также методы и средства защиты локальных и корпоративных сетей от удаленных Internet-атак. Особое внимание уделяется проблемам обеспечения информационной безопасности электронного бизнеса и электронной коммерции. Формулируется концепция информационной безопасности и определяется политика безопасности в сетях.

Анализируются технологии защиты данных, базовые технологии сетевой безопасности, обнаружения вторжений и управления сетевой безопасностью. В частности, рассматриваются принципы, алгоритмы и протоколы современных криптографических средств защиты информации; описываются различные типы межсетевых экранов и даются рекомендации по их использованию; обсуждаются методы и средства формирования криптозащищенных виртуальных туннелей через открытые коммуникации глобальных открытых сетей типа Internet; рассматриваются вопросы обеспечения удаленного доступа к информационным ресурсам предприятия; описываются задачи защиты информации в сетях передачи данных и пути их решения; излагаются концепция беспроводной сети, угрозы на безопасность беспроводной сети, проблемы безопасности беспроводной сети; анализируются методы и системы управления сетевой безопасностью.

На основе анализа и управления рисками, формулируется методология построения системы информационной безопасности предприятия.

Пособие рассчитано на студентов высших учебных заведений, а также лицам, занимающимся в области информационной технологий и компьютерных систем.

The given manual is devoted to actual problems of protection of the information at creation and use of computer networks and corporate information systems. Kinds of attacks to computer networks and systems, and also methods and means of protection of local and corporate networks from the removed Internet-attacks are discussed. The special attention is given problems of maintenance of information safety of electronic business and electronic commerce. The concept of information safety is formulated and the politics of safety in networks is determined.

***

Technologies of protection of data, base technologies of network safety, detection of intrusions and managements of network safety are analyzed. In particular, principles, algorithms and reports of modern cryptographic means of protection of the information are considered; various types of gateway screens are described and recommendations on their use are given; methods and means of formation cryptoprotection virtual tunnels through the open communications of the global open networks of type Internet are discussed; questions of maintenance of the removed access to information resources of the enterprise are considered; problems of protection of the information in networks of data transmission and a way of their decision are described; the concept of a wireless network, threat on safety of a wireless network, a problem of safety of a wireless

network are stated; methods and control systems of network safety are analyzed.

On the basis of the analysis and management of risks, the methodology of construction of system of information safety of the enterprise is formulated.

The manual is calculated on students of higher educational institutions, and also to the persons who are engaged in the field of information technologies and computer systems.

Тақризчилар: акад. **Бекмуратов Т.Ф.** – Замонавий ахборот технологиялари ИТМ, «Алгоритм-инжиниринг» ИТИ етакчи илмий ходими, т.ф.д., проф;
проф. **Орипов М.М.** – Мирзо Улуғбек номли Ўзбекистон Миллий университети «Информатика ва татбиқий дастурлаш» кафедраси мудири, физика-математика фанлари доктори.

ISBN 978-9943-326-20-0

МУНДАРИЖА