INFOTEHNOLOOGIA
Turbemeetodid
Küberturbe juhised

Information technology
Security techniques
Guidelines for cybersecurity
(ISO/IEC 27032:2012, identical)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO/IEC 27032:2018 „Infotehnoloogia. Turbemeetodid. Küberturbe juhised“ sisaldab rahvusvahelise standardi ISO/IEC 27032:2012 „Information technology. Security techniques. Guidelines for cybersecurity“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 27032:2018 consists of the identical English text of the International Standard ISO/IEC 27032:2012 „Information technology. Security techniques. Guidelines for cybersecurity“.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian Standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 27032:2018 on jõustunud sellekohase teate avaldamisega EVS Teataja 2018. aasta veebruarikuu numbris.	Standard EVS-ISO/IEC 27032:2018 has been endorsed with a notification published in the February 2018 issue of the official bulletin of the Estonian Centre for Standardisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See standard annab juhiseid küberturvalisuse seisundi täiustamiseks, tuues esile selle tegevuse ainuomased tahud ning ta sõltuvused muudest turbealadest, sealhulgas

— infoturbest,

— võrguturbest,

— võrgustikuturbest,

— elutähtsa teabetaristu kaitsest (CIIP).

Standard hõlmab riskiosaliste etalonturbe tavasid küberruumis, andes

— ülevaate küberturbest,

— ühe seletuse küberturbe ja muude turbeliikide vahelise seose kohta,

— riskiosaliste määratluse ja nende küberruumirollide kirjelduse,

— juhiseid üldiste küberturvaküsimuste käsitluseks,

— ühe karkassi, millega võimaldada riskiosaliste koostööd küberturvaküsimuste lahendamisel.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks. However there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices as there are gaps between these domains, as well as a lack of communication between organizations and providers in the Cyberspace. This is because the devices and connected networks that have supported the Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for the Cyberspace.

As such, the first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

— social engineering attacks;

— hacking;

— the proliferation of malicious software (“malware”);

— spyware; and

— other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

— preparing for attacks by, for example, malware, individual miscreants, or criminal organizations on the Internet;

— detecting and monitoring attacks; and

— responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned. Many of these stakeholders can reside in different geographical locations and time zones, and are likely to be governed by different regulatory requirements. Stakeholders include:

— consumers, which can be various types of organizations or individuals; and

— providers, which include service providers.

Thus, this International Standard also provides a framework for

— information sharing,

— coordination, and

— incident handling.

The framework includes

— key elements of considerations for establishing trust,

— necessary processes for collaboration and information exchange and sharing, as well as

— technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.

Information technology — Security techniques — Guidelines for cybersecurity

1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

— information security,

— network security,

— internet security, and

— critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

— an overview of Cybersecurity,

— an explanation of the relationship between Cybersecurity and other types of security,

— a definition of stakeholders and a description of their roles in Cybersecurity,

— guidance for addressing common Cybersecurity issues, and

— a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

2 Applicability

2.1 Audience

This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

2.2 Limitations

This International Standard does not address:

— Cybersafety,

— Cybercrime,

— CIIP,

— Internet safety, and

— Internet related crime.

It is recognized that relationships exist between the domains mentioned and Cybersecurity. It is, however, beyond the scope of this International Standard to address these relationships, and the sharing of controls between these domains.

It is important to note that the concept of Cybercrime, although mentioned, is not addressed. This International Standard does not provide guidance on law-related aspects of the Cyberspace, or the regulation of Cybersecurity.

The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints. However, the extension of the Cyberspace to other spatial representations through communication media and platforms are not addressed, nor the physical security aspects of them.

EXAMPLE 1 Protection of the infrastructure elements, such as communications bearers, which underpin the Cyberspace are not addressed.

EXAMPLE 2 The physical security of mobile telephones that connect to the Cyberspace for content download and/or manipulation is not addressed.

EXAMPLE 3 Text messaging and voice chat functions provided for mobile telephones are not addressed.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply.

4.1
adware
application which pushes advertising to users and/or gathers user online behaviour

NOTE The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software.

4.2
application
IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

[ISO/IEC 27034-1:2011]

4.3
application service provider
operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models

EXAMPLE Online game operators, office application providers and online storage providers.

4.4
application services
software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications

4.5
application software
software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself

[ISO/IEC 18019]