Институт специальной связи и защиты информации
НТУУ «КПИ»

Семейство стандартов ISO/IEC 27000 как источник для создания национального стандарта по кибербезопасности

Заместитель заведующего СК№2
полковник Госспецсвязи Бакалинский А.О.
т. 0674445199 e-mail: baov@meta.ua
Начальник лаборатории СК № 5
подполковник Госспецсвязи Безштанько В.М.
т. 067 4446682 e-mail: v.bezshtanko@gmail.com

ISO/IEC 27000:2014

Терминология

27000
Обзор и словарь

Основные требования

27009
Требования по применению ISO/IEC 27001

27001
Системы управления информационной безопасностью. Требования

27006
Требования к органам аудита и сертификации систем управления информационной безопасностью

Основные руководства

27002
Практические правила управления информационной безопасностью

27003
Руководство по внедрению Системы управления информационной безопасности

27004
Измерение эффективности системы управления информационной безопасностью

TR 27016
Организационная рентабельность управления информационной безопасностью

TR 27008
Руководство по контролю аудита ISMS

27007
Руководство для аудита систем менеджмента информационной безопасности

27005
Управление рисками информационной безопасности

27013
Руководство по внедрению ISO/IEC 27000 и ISO/IEC 20000-1

27035
Управление инцидентами безопасности

27037 Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств

Узконаправленные руководства

27011
Руководство по управлению информационной безопасностью для телекоммуникационных организаций на основе ISO/IEC 27002

27799
Информатизация здравоохранения – управление информационной безопасности в здравоохранении используя ISO/IEC 27002

27017, 27018, 27019, 27033, 27034, 27039, 27040-27044

27010
Руководство по управлению информационной безопасностью для межсекторных и межорганизационных коммуникаций

27015
Руководство по управлению информационной безопасностью для финансовых сервисов

27032
Руководство по кибербезопасности

Легенда: :
Нормативный стандарт
Информативный стандарт
Поддержка

СЕРИЯ ISO/IEC 27000

International Organization for Standardization

- **ISO/IEC 27000:2014** Information technology. Security techniques. Information security management systems. Overview and vocabulary - Определения и основные принципы.

- **ISO/IEC 27001:2013** Information technology. Security techniques. Information security management systems. Requirements - Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

- **ISO/IEC 27002:2013** Information technology. Security techniques. Code of practice for information security management - Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.

- **ISO/IEC 27003:2010** Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance - Руководство по внедрению системы управления информационной безопасностью.

- **ISO/IEC 27004:2009** Information technology. Security techniques. Information security management. Measurement - Измерение эффективности системы управления информационной безопасностью.

IEC

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27005:2011** Information technology. Security techniques. Information security risk management - Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности.

- **ISO/IEC 27006:2011** Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems -Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью.

- **ISO/IEC 27007:2011** Information technology. Security techniques. Guidelines for Information Security Management Systems auditing - Руководство для аудитора СУИБ.

- **ISO/IEC TR 27008:2011** Information technology. Security techniques. Guidance for auditors on ISMS controls - Руководство по аудиту механизмов контроля СУИБ. Служит дополнением к стандарту ISO 27007.

- **ISO/IEC 27009** Information technology. Security techniques. Application of ISO/IEC 27001 – Reguirements (DRAFT). – Требования по применению ISO/IEC 27001.

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27010:2012 Information technology. Security techniques. Information security management for inter-sector communications - Управление информационной безопасностью при коммуникациях между секторами. Стандарт состоит из нескольких частей, предоставляющих руководство по совместному использованию информации о рисках информационной безопасности, механизмах контроля, проблемах и/или инцидентах, выходящей за границы отдельных секторов экономики и государств, особенно в части, касающейся "критичных инфраструктур".**

- **ISO/IEC 27011:2008** Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 - Руководство по управлению информационной безопасностью для телекоммуникаций.

- **ISO/IEC 27013:2012** IT Security. Security techniques. Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001 - Руководство по интегрированному внедрению ISO 20000 и ISO 27001.

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27014:2013** Information technology. Security techniques. Information security governance framework - Базовая структура управления информационной безопасностью.

- **ISO/IEC TR 27015:2012** Information technology. Security techniques. Information security management systems guidelines for financial and insurance sectors - Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе.

- **ISO/IEC TR 27016:2012** Information technology. Security techniques. Information security management. Organizational economics . Экономика предприятия.

- **ISO/IEC 27017** Information technology. Security techniques. Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 (DRAFT) - Руководство по управления информационной безопасности при использовании услуг облачных вычислений.

- **ISO/IEC 27018** Information technology. Security techniques. Code of practice for PII protection in public clouds acting as PII processors (DRAFT) - Свод практических правил для защиты PII в общественных облаках, выступающих в качестве процессоров PII.

СЕРИЯ ISO/IEC 27000

- **ISO/IEC TR 27019:2013** Information technology. Security techniques. Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. - Руководство по внедрению систем управления информационной безопасностью в секторе энергетики.

- **ISO/IEC 27031:2011** Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity - Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса.

- **ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity - Руководство по обеспечению кибербезопасности.**

- **ISO 27033** стандарт сетевой безопасности. 1-3,5 части приняты Проекты частей 4,6,7 ISO 27033 находятся в разной стадии готовности.

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27034** Information technology. Security techniques. Application security - Безопасность приложений. Состоит из 6 частей. Проекты различных частей стандарта ISO 27034 находятся в различной стадии разработки.

- **ISO/IEC 27035:2011** Information technology. Security techniques. Security incident management - Управление инцидентами безопасности.

- **ISO/IEC 27036-3:2013** IT Security. Security techniques. Guidelines for security of outsourcing - Руководство по аутсорсингу безопасности.

- **ISO/IEC 27037:2012 IT Security. Security techniques. Guidelines for identification, collection and/or acquisition and preservation of digital evidence - Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств.**

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27038 Information technology. Security techniques. Specification for digital redaction (FINAL DRAFT) - Спецификация для цифрового редактирования.**

- **ISO/IEC 27039** Information technology. Security techniques. Selection, deployment and operations of intrusion detection and prevention systems (IDPS) (DRAFT) - Выбор, развертывание и функционирование системы обнаружения и предотвращения вторжений.

- **ISO/IEC 27040** Information technology. Security techniques. Storage security (DIS) – Безопасное хранение данных.

- **ISO/IEC 27041 Information technology. Security techniques. Assurance for digital evidence investigation methods (DRAFT) - Обеспечение цифровых методов доказательства для следствия.**

СЕРИЯ ISO/IEC 27000

- **ISO/IEC 27042 Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence (DRAFT) - Руководящие принципы для анализа и интерпретации цифровых доказательств.**

- **ISO/IEC 27043 Information technology. Security techniques. Incident investigation principles and processes (DRAFT) – Расследование инцидентов, принципы и процессы.**

- **ISO/IEC 27044** Information technology. Security techniques. Guidelines for security information and event management (SIEM) (DRAFT) - Руководство по информационной безопасности и управлению событиями.

- **ISO 27799:2008** Health informatics. Information security management in health using ISO/IEC 27002 - Управление информационной безопасностью в сфере здравоохранения.

Общая характеристика стандарта ISO/IEC 27032:2012

- Стандарт опубликован – в июне 2012 года.
- Напечатан на 58 страницах.
- Состоит из 13 разделов и 3-х приложений.
- Использует 53 термина (39 впервые), из которых:

a) 4 – приведены из ISO/IEC 27000:2012,

b) 3 – адаптированы из ISO/IEC 27000:2012,

c) 7 – приведены из других стандартов.

СТРУКТУРА СТАНДАРТА

1.СФЕРА ДЕЯТЕЛЬНОСТИ

2.ОБЛАСТЬ ПРИМЕНЕНИЯ

3.СПРАВОЧНЫЕ ДОКУМЕНТЫ

4.ОПРЕДЕЛЕНИЯ И ХАРАКТЕРИСТИКИ

5. СПИСОК СОКРАЩЕНИЙ

6. ОБЩИЕ СВЕДЕНИЯ

7. ПРИЧАСТНЫЕ ЛИЦА В КИБЕРПРОСТРАНСТВЕ

8. РЕСУРСЫ В КИБЕРПРОСТРАНСТВЕ

9. УГРОЗЫ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

10. РОЛИ ПРИЧАСТНЫХ ЛИЦ В КИБЕРПРОСТРАНСТВЕ

11. НАСТАВЛЕНИЕ ДЛЯ ПРИЧАСТНЫХ ЛИЦ

12. СИСТЕМЫ УПРАВЛЕНИЯ В КИБЕРПРОСТРАНСТВЕ

13. СТРУКТУРА РАСПРОСТРАНЕНИЯ И ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИИ

ISO/IEC 27032

Руководство по обеспечению кибербезопасности

Приложение А (информативное) Состояние готовности кибербезопасности

Приложение В (информативное) Дополнительные источники

Приложение С (информативные) Примеры сопутствующих документов

Введение

Киберпространство - сложная среда, возникающая в процессе взаимодействия людей, программного обеспечения и предоставляемых Интернет-услуг Интернет, которые поддерживаются международными распределенными физическими информационно-коммуникационными технологиями (ИКТ), устройствами и связанными сетями.

Однако существуют проблемы безопасности, которые не покрываются текущими передовыми методами в сфере информационной безопасности, интернет безопасности, сетевой безопасности и ИКТ безопасности за счет недоработок в данных сферах, а так же за счет недостатка связи между организациями и поставщиками в киберпространстве.

Причины отсутствия взаимодействия:

-у устройств и связанных сетей, которые поддерживаются в киберпространстве, есть большое количество владельцев со своими бизнес - операционными и регулирующими особенностями;

-каждая организация и поставщики услуг преследуют свои цели в киберпространстве в конкретных сферах безопасности;

-фрагментированное состояние безопасности в киберпространстве.

Сфера, рассматриваемая стандартом

Первой задачей, которую должен решить данный Международный стандарт, является обеспечение безопасности в киберпространстве или устранение проблем кибербезопасности, которые возникают вследствие наличия пробелов между различными сферами безопасности в киберпространстве (работа «на меже»).

Стандарт предоставляет собой **техническое руководство,** которое имеет целью предотвращение реализации наиболее распространенных рисков кибербезопасности, включая:

- социальный инжиниринг;
- взлом;
- быстрое распространение вредоносного ПО;
- программы-шпионы; и
- другое потенциально нежелательное ПО.

Сфера, рассматриваемая стандартом

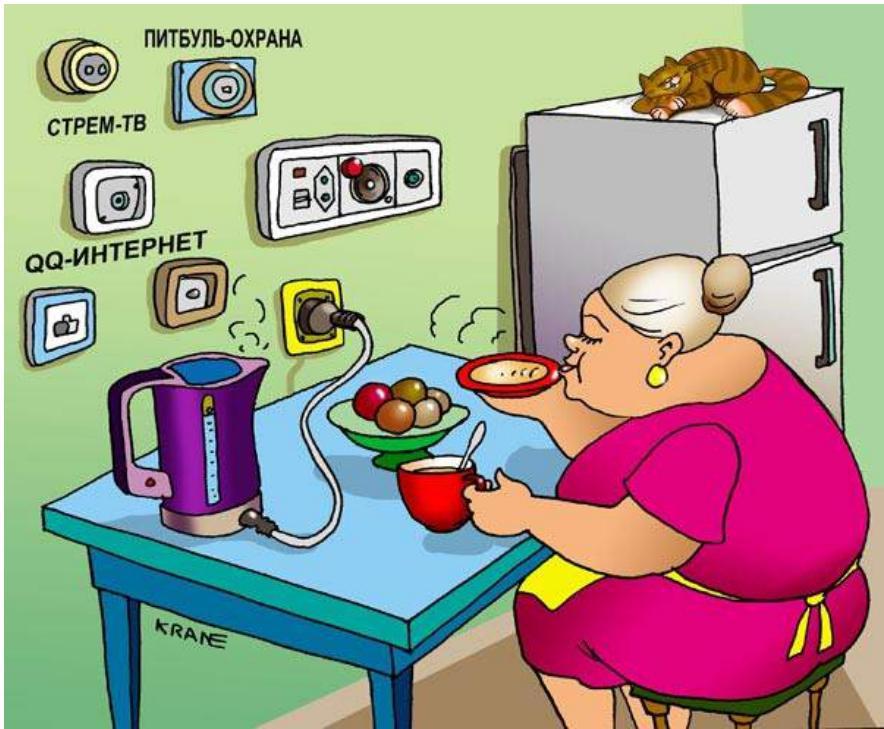
Вторая задача, на решение которой направлен стандарт, - **сотрудничество**, поскольку существует потребность в действенном и эффективном информационном обмене, координации и обработке инцидентов среди лиц, которые причастны к киберпространству.

Это сотрудничество должно вестись безопасным и надежным способом, который также защищает конфиденциальность заинтересованных частных лиц. Многие из этих заинтересованных лиц могут находиться в географически различных местах и часовых поясах, и их деятельность регулируется различными нормативными требованиями, которые определяются национальными законодательствами стран.

Заинтересованные лица

Заинтересованные (причастные) лица:

- пользователи (потребители), которые могут быть различными типами организаций или частными лицами; и
- поставщики, среди которых поставщики услуг.



Сфера деятельности

Международный стандарт обеспечивает:

- разъяснение общих положений кибербезопасности,

- объяснение связи между кибербезопасностью и другими типами безопасности,

- определение заинтересованных (причастных) лиц и описание их ролей в кибербезопасности,

- руководство по основным вопросам в кибербезопасности,

- рекомендации по организации структуры, с помощью которой можно реализовать сотрудничество заинтересованных лиц для решения вопросов относительно обеспечения Кибербезопасности.

Область применения

Аудитория:

- поставщики
- потребители.

Организации, которые предоставляют услуги в Киберпространстве людям для использования в домашних условиях или другим организациям, вероятно, должны подготовить руководство, основанное на этом Международном стандарте, который содержит дополнительные объяснения и примеры, которых достаточно, чтобы читатель смог понять и действовать согласно данному руководству.

Ограничения

- Киберзащищенность,
    - Киберпреступление,
    - защита критической информационной инфраструктуры,
    - Интернет защищенность,
    - преступления, связанные с Интернетом

Термины и определения

…

4.18 Киберпреступность

Преступная деятельность, где службы или приложения в Киберпространстве используются или являются целью преступления, или где Киберпространство является источником, инструментом, целью, или местом преступления.

ы и определения

4.19 Киберзащищенность

Состояние защищенности от физических, социальных, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов или последствий отказа, повреждения, ошибки, несчастных случаев, вреда или любых других случаев в Киберпространстве, которые можно считать нежелательными.

ПРИМЕЧАНИЕ 1. Может иметь отношение к людям или активам и проявляться в форме защищенности от событий или воздействия чего-либо, что может привести к ущербу здоровью, моральному вреду или экономическим потерям.

2. В основном, защищенность определяется как стабильное состояние, при ибо не будут вызваны неблагоприятные эффекты.

Термины и определения

4.20 Кибербезопасность, безопасность в киберпространстве

Сохранение конфиденциальности, целостности и доступности информации в Киберпространстве.

ПРИМЕЧАНИЕ 1. Кроме того, другие свойства, такие как подлинность, контролируемость, безотказность, и надежность также могут быть включены в список.

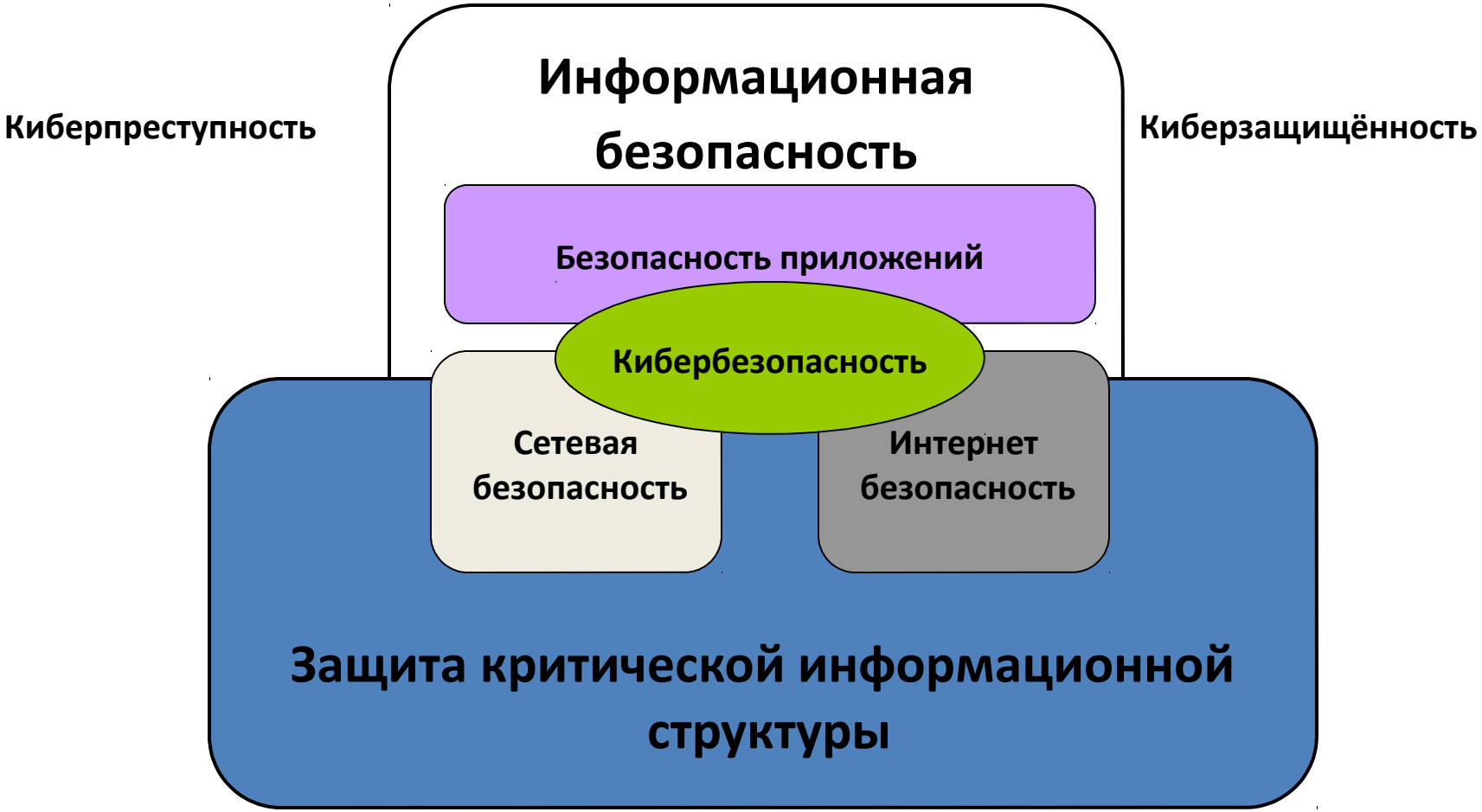
ПРИМЕЧАНИЕ 2. Адаптировано исходя из определения информационной безопасности в ISO/IEC 27000:2009.

4.21 Киберпространство

Сложная среда, возникающая в процессе взаимодействия людей, программного обеспечения и предоставляемых Интернет-услуг Интернет, посредством технологических устройств или объединенных сетей, которая не существует в любой физической форме.

….

Связь между кибербезопасностью и другими сферами безопасности



Состояние законодательной базы Украины сегодня

Инициаторами создания различных вариантов проектов закона на сегодняшний день являются МВД, СБ Украины, ГСССЗИ Украины, депутатские группы.

Проект Закона «Про внесение изменений к Закону Украины “Про основы национальной безопасности Украины” дает определение только двум понятиям:

- “**кібернетична безпека** (кібербезпека) — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;
- **кібернетичний простір** (кіберпростір) — середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем”.

Таким образом, предлагаемое определение кибернетического пространства исключает человека из круга факторов, которые образовывают кибернетическое пространство, являясь одновременно основным источником кибернетических рисков.

?

ВЫВОДЫ

1.НЕОБХОДИМО поддержать принятие Проекта Закона «Про внесение изменений к Закону Украины “Про основы национальной безопасности Украины”.

2.Инициировать начало работы по созданию **стратегии кибернетической безопасности** Украины, создав рабочую группу из ведущих экспертов ГСССЗИ, СБУ, МВД, СВР, МО, НАНУ.

3.Организовать **межведомственный центр компетенции** в сфере кибербезопасности промышленных предприятий и объектов критической инфраструктуры.

4.Создать условия для **оперативного взаимодействия** экспертов кибербезопасности из различных структур, к примеру путем создания рабочей, консультативной группы при РНБО.

5.Организация **вневедомственного механизма мониторинга и прогнозирования** угроз кибернетической безопасности в Украине.

ВЫВОДЫ

6. Внести изменение в Постановление КМУ №787 от 27.08.2010 г., добавив в области знаний "1701 Информационная безопасность" **специальность для подготовки специалиста, магистра - «Кибернетическая безопасность»**, предусмотрев возможность поступления на нее бакалавров из разных областей знания: «Информационная безопасность», «Компьютерные науки», «Право», путем введения соответствующих специализаций.

7. Для подготовки специалиста, магистра по специальности «Кибернетическая безопасность» установить соотношение преподаватель-обучаемый **1:5** (исключительно! ГСССЗИ Украины, СБ Украины, СВР Украины, МВД, МОУ). Для этого внести необходимые изменения в Постановление КМУ № 1134 от 17.08.2002 г.

Project Data

Title: "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains"

Project Number: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR

Duration: 3 years (01/12/2013-01/12/2016)

Total Budget: 725 746,76 Euro

Grant Holder: Tallinn University of Technology, Estonia

Preliminary matrix of responsibility

ID	Course	UA Developers	UA Experts	EU Experts
Master courses				
CM-1	Foundations of Dependability and Security	Lead developer: KhAI Contributor: TNTU	RPC Radiy	KTH
CM-2	System and Networks Security and Resilience	Lead developer: ISC Contributor: SIB	USIF	CityU
CM-3	Human Factors Engineering	Lead developer: KhAI Contributor: TI	RPC Radiy	KTH
CM-4	Risk Analysis of SoS Security and Resilience	Lead developer: TI Contributor: KhAI	USIF	CityU
CM-5	Secure and Resilient PLD-Based Systems	Lead developer: TNTU Contributor: KhAI	RPC Radiy	TUT
Doctoral courses				
CP-1	Formal Methods for System Security and Resilience	Lead developer: KhNU Contributor: KhAI	RPC Radiy	CINI
CP-2	Security of Evolvable (Web, Cloud) Systems	Lead developer: KhAI Contributor: KhNU	USIF	KTH
CP-3	Security Management Systems	Lead developer: DNU Contributor: ISC	USIF	IICT
In-service training modules				
CT-1	Technologies of Networks Security Assessment	Lead developer: SIB Contributor: ISC	USIF	CINI
CT-2	Technologies of FPGA Security and Resilience	Lead developer: KhAI Contributor: TNTU	RPC Radiy	TUT
CT-3	Security Assurance Cases	Lead developer: KhAI Contributor: DNU	RPC Radiy	IICT

Спасибо за внимание!