Регуляторная практика обеспечения безопасности промышленных систем

Profit Security Day

Апрель 2021

ISACA
Nur-Sultan Chapter

Кто мы?

Кто мы?

Об ISACA

Об ISACA

ISACA® (isaca.org) приблизилась к 50-летию своего существования. Это глобальная ассоциация, помогающая частным лицам и предприятиям реализовать весь потенциал технологий. Сегодняшний мир основан на технологиях, и ISACA вооружает профессионалов знаниями, квалификацией, образованием и обществом, чтобы продвигаться по карьерной лестнице и преобразовывать свои организации.

ISACA использует опыт своих 450 000 вовлеченных профессионалов в области информационной и кибербезопасности, управления, аудита, рисков и инноваций, а также своей дочерней компании CMMI® Институт для продвижения инноваций с помощью технологий. ISACA представлена в 188 странах, в том числе в 220 отделениях по всему миру и офисах в США и Китае.

ISACA

Факты и цифры

Основана: 1969 г.
Количество участников: более 135,000 в 188 странах
Количество сертифицированных специалистов: 165,000+
Количество чаптеров: 220

ISACA сертификации

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Control Objectives for Information and Related Technology (COBIT) 5
- Certified in Risk and Information Systems Control (CRISC)
- Cybersecurity Nexus Practitioner (CSX-P)

CISA Certified Information Systems Auditor
CRISC Certified in Risk and Information Systems Control
CISM Certified Information Security Manager
CGEIT Certified in the Governance of Enterprise IT
CSX CYBERSECURITY NEXUS
COBIT 2019
ISACA Nur-Sultan Chapter

Кто мы?

Об ISACA Nur-Sultan Chapter

- В ноябре 2016 мы получили разрешение открыть отделение у ISACA® и в феврале 2017 года официально зарегистрировали Общественное Объединение «ИСАКА Астана» (переименованное в «ИСАКА Нур-Султан Чаптер»)
- Мы состоим из более полусотни участников из самых разных отраслей. Члены сообщества являются профессионалами в области ИТ, аудита и кибербезопасности, и работают в крупнейших организациях Республики Казахстан, национальных компаниях и филиалах западных компаний
- Поддержка, предоставляемая партнерами неоценима и жизненно важна для нашей некоммерческой организации, т.к. мы состоим из волонтеров, работающих на безвозмездной основе. Особое внимание мы уделяем молодежи. Члены нашего сообщества, опытные специалисты в области ИТ, аудита и кибербезопасности проводят бесплатные факультативные лекции в университетах и т.д.
- Мы открыты новым участникам и намерены в дальнейшем активно расширяться


ISACA
Trust in, and value from, information systems

Information Systems Audit and Control Association
Chapter Charter

Pursuant to the authority vested in the Board of Directors of the Information Systems Audit and Control Association, this 235th Chapter Charter is hereby granted to the:

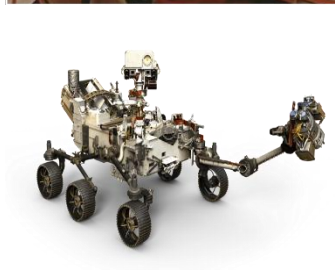
Astana Chapter

with authority to exercise all requisite rights and responsibilities as set forth in the Information Systems Audit and Control Association Bylaws.

Approved this 3rd day of November, 2016.

Attest:

Christos K. Dimitriadis
2016-2017 International Chair



65 членов ISACA Nur-Sultan Chapter (по состоянию на 30.03.2021)

Из них обладатели сертификатов:

30	CISA
11	CISM
2	CGEIT
5	CRISC
7	CDPSE

ISACA Nur-Sultan Chapter

Информационные технологии и промышленные системы

Информационные технологии и промышленные системы

Атрибут	ИТ	Промышленные системы
Конфиденциальность	Высокий	Низкий
Целостность	Низкий-Средний	Очень высокий
Доступность	Низкий-Средний	Очень высокий
Аутентификация	Средний-Высокий	Высокий
Неотрекаемость	Высокий	Низкий-Средний
Критичность по времени	Несколько дней	Критично
Простой системы	Терпимо	Неприемлемо
Навыки безопасности / Осведомленность	Обычно хорошо	Обычно плохо
Жизненный цикл системы	3-5 лет	15-25 лет
Интеграция	Не критично	Критично
Вычислительные ресурсы	Без лимитные	Очень ограничены старыми процессорами
Изменения программного обеспечения	Часто	Редко
Последствия наихудшего случая	Потеря данных	Поломки оборудования | Происшествия

ISACA Nur-Sultan Chapter

Регуляторная практика

Республика Казахстан

Закон «Об информатизации»

Критически важные объекты информационно-коммуникационной инфраструктуры – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, «электронного правительства».

Негосударственные информационные системы, отнесенные к критически важным объектам информационно-коммуникационной инфраструктуры, а также предназначенные для формирования государственных электронных информационных ресурсов, приравниваются к информационным системам государственных органов в части соблюдения требований по обеспечению информационной безопасности.

Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности

Положения ЕТ, относящиеся к сфере обеспечения информационной безопасности, обязательны для применения государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры.

Примеры требований:

- *Серверное оборудование АПК и системы хранения данных размещаются в серверном помещении*
- *Двери серверного помещения составляют не менее 1,2 метра в ширину и 2,2 метра в высоту*
- *На этапе опытной и промышленной эксплуатации объектов информатизации используются средства и системы:*
  - *обнаружения и предотвращения вредоносного кода;*
  - *мониторинга и управления инцидентами и событиями ИБ;*
  - *обнаружения и предотвращения вторжений*

ISACA Nur-Sultan Chapter

Соединенные Штаты Америки

Понятие кибербезопасности операционных технологий, применяемых в стратегических объектах, изначально было определено в США и именно там были разработаны программы защиты операционных технологий стратегических объектов. В 1998 году в США была издана директива по вопросу о защите стратегически важной инфраструктуры. Данный документ определил национальную инфраструктуру, имеющую критическое значение для национальной и экономической безопасности. В данной директиве были определены меры, которые необходимо было принять **для обеспечения кибербезопасности операционных технологий, используемых на стратегических объектах**.

Регуляторные акты:

- Май 2017, Исполнительный приказ 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- Апрель 2018, *Framework for Improving Critical Infrastructure Cybersecurity version 1.1*

Function
Identify
Protect
Detect
Respond
Recover

ISACA Nur-Sultan Chapter

Европейский союз

Набор директив направленный на кибербезопасность стратегических объектов. Директива 2008/114/EC от 8 Декабря 2008 года, направленная на выявление и назначение стратегических объектов Европы и оценка необходимости повышения их безопасности.

(14) The efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of ECIs and the Member States, and between the Member States and the Commission. Each Member State should collect information concerning ECIs located within its territory. The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of ECIs, where necessary.

List of ECI sectors

Sector	Subsector	
I Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
II Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short-sea shipping and ports	

The identification by the Member States of critical infrastructures which may be designated as ECIs is undertaken pursuant to Article 3. Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector.

ISACA Nur-Sultan Chapter

Вопросы и ответы

Q&A

ISACA
Nur-Sultan Chapter