Kaspersky Industrial Cybersecurity Conference

Обеспечение кибербезопасности АЭС на основе дифференцированного/ риск-ориентированного подходов

Екатерина Рудина
Семен Корт
Денис Бабаев

Kaspersky ICS CERT

kaspersky

Kaspersky Industrial Cybersecurity Conference

Обеспечение кибербезопасности АЭС

Екатерина Рудина
Семен Корт
Денис Бабаев

Kaspersky ICS CERT

kaspersky

Зачем и почему нужен этот проект

Выполнение требований регулятора

– необходимое условие лицензирования на строительство АЭС

Безопасность by design

– проектирование кибербезопасности как неотъемлемого свойства критически важного объекта

Цели безопасности

Поддержка ядерной безопасности (safety)

Поддержка ядерной физической безопасности (security)

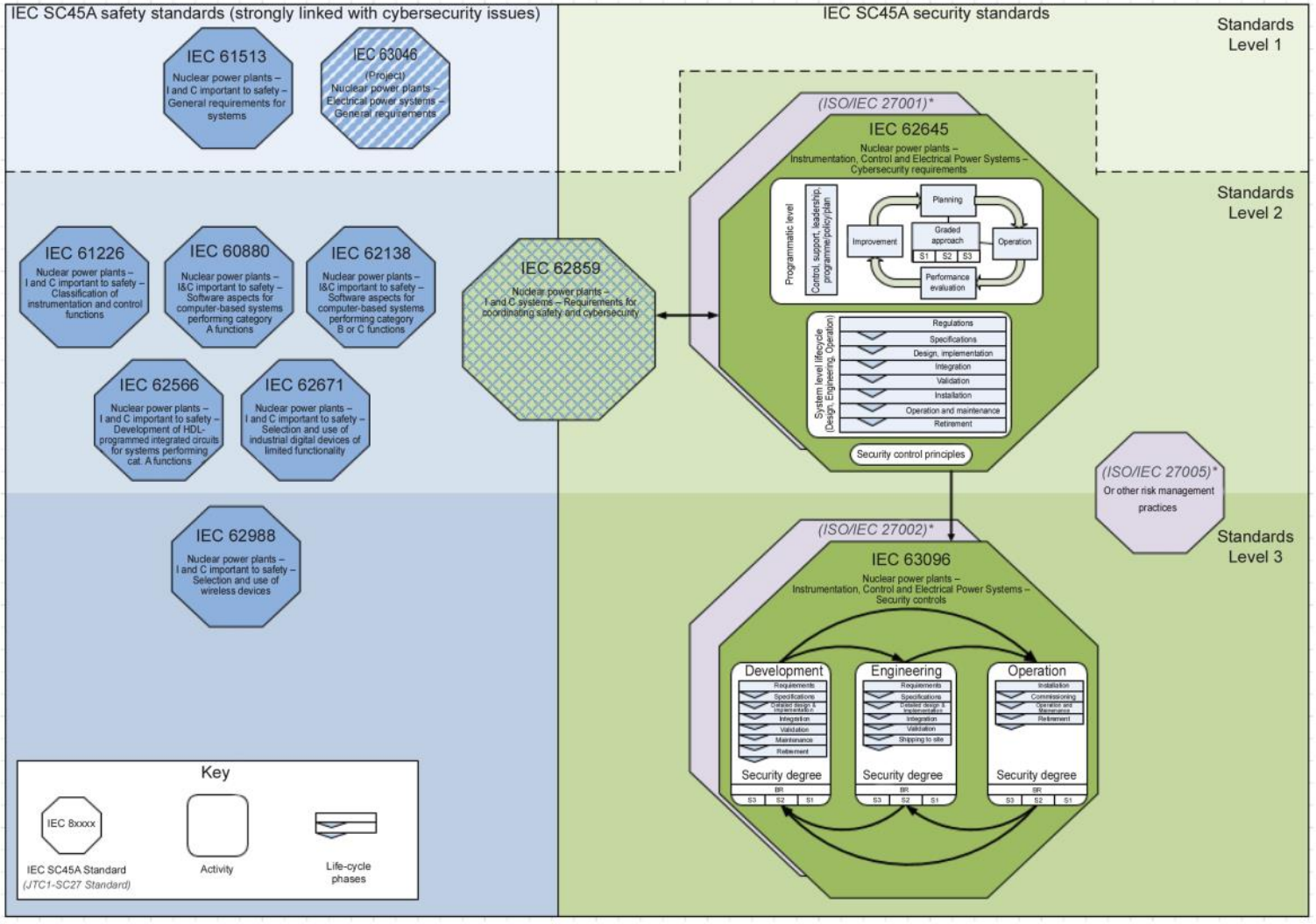
Информационная безопасность (конфиденциальность, целостность, доступность)

Кибербезопасность АСУ ТП

Использование двух основных подходов

Дифференцированный
применение мер безопасности пропорционально потенциальным последствиям атаки

Риск-ориентированный
на основе оценки риска как сочетания вероятности события и тяжести его последствий


IEC SC45A safety standards (strongly linked with cybersecurity issues)
IEC SC45A security standards
Standards Level 1
Standards Level 2
Standards Level 3
IEC 61513
Nuclear power plants – I and C important to safety – General requirements for systems
IEC 63046
(Project)
Nuclear power plants – Electrical power systems – General requirements
IEC 61226
Nuclear power plants – I and C important to safety – Classification of instrumentation and control functions
IEC 60880
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category A functions
IEC 62138
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category B or C functions
IEC 62566
Nuclear power plants – I and C important to safety – Development of HDL-programmed integrated circuits for systems performing cat. A functions
IEC 62671
Nuclear power plants – I and C important to safety – Selection and use of industrial digital devices of limited functionality
IEC 62988
Nuclear power plants – I and C important to safety – Selection and use of wireless devices
IEC 62859
Nuclear power plants – I and C systems – Requirements for coordinating safety and cybersecurity
(ISO/IEC 27001)*
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Programmatic level
Control, support, leadership, programme/policy plan
Planning
Graded approach
Operation
Performance evaluation
Improvement
S1
S2
S3
System level lifecycle (Design, Engineering, Operation)
Regulations
Specifications
Design, implementation
Integration
Validation
Installation
Operation and maintenance
Retirement
Security control principles
(ISO/IEC 27005)*
Or other risk management practices
(ISO/IEC 27002)*
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
Development
Engineering
Operation
Requirements
Specifications
Detailed design & implementation
Integration
Validation
Maintenance
Retirement
Shipping to site
Installation
Commissioning
Operation and Maintenance
Security degree
BR
Key
IEC 8xxxx
IEC SC45A Standard
(JTC1-SC27 Standard)
Activity
Life-cycle phases

Магическое число 2

(на самом деле 3)

2 подхода:
дифференцированный и риск-ориентированный
(+совмещенный)

2 уровня рассмотрения:
уровень станции и уровень систем
(+ уровень архитектуры)

2 модели для оценки рисков:
функциональная модель + модель на основе MITRE Att&ck
(+ сценарии)

Дифференцированный подход

Применение мер безопасности пропорционально потенциальным последствиям атаки

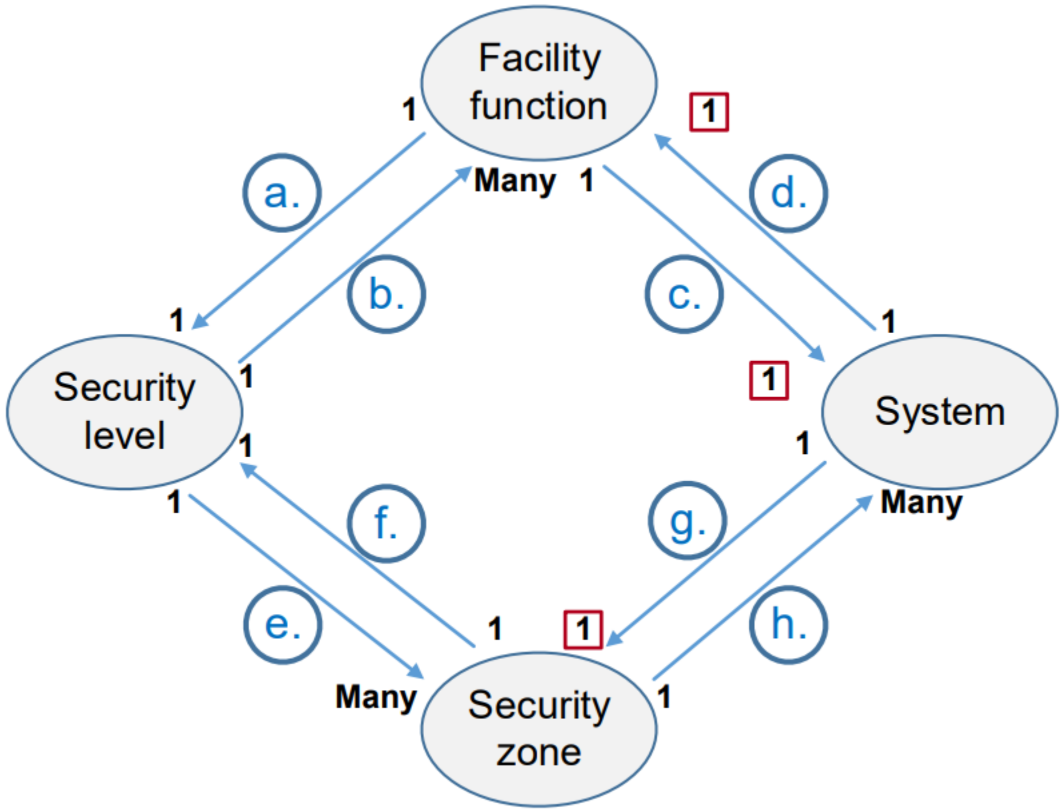
Дифференцированный подход

Применяется в целом к управлению рисками в атомной отрасли

Меры защиты принимаются пропорционально возможному ущербу

Для реализации подхода системы и цифровое оборудование разделены на зоны на основе анализа и оценки рисков

К каждой зоне применяется комплекс мероприятий в соответствии со степенью требуемой защищенности систем зоны


Facility function
Security level
System
Security zone
a.
b.
c.
d.
e.
f.
g.
h.
1
Many
1
1
1
1
1
1
1
1
Many
1
1
Many
1
1
1

Риск-ориентированный подход

На основе оценки риска по ISO27005

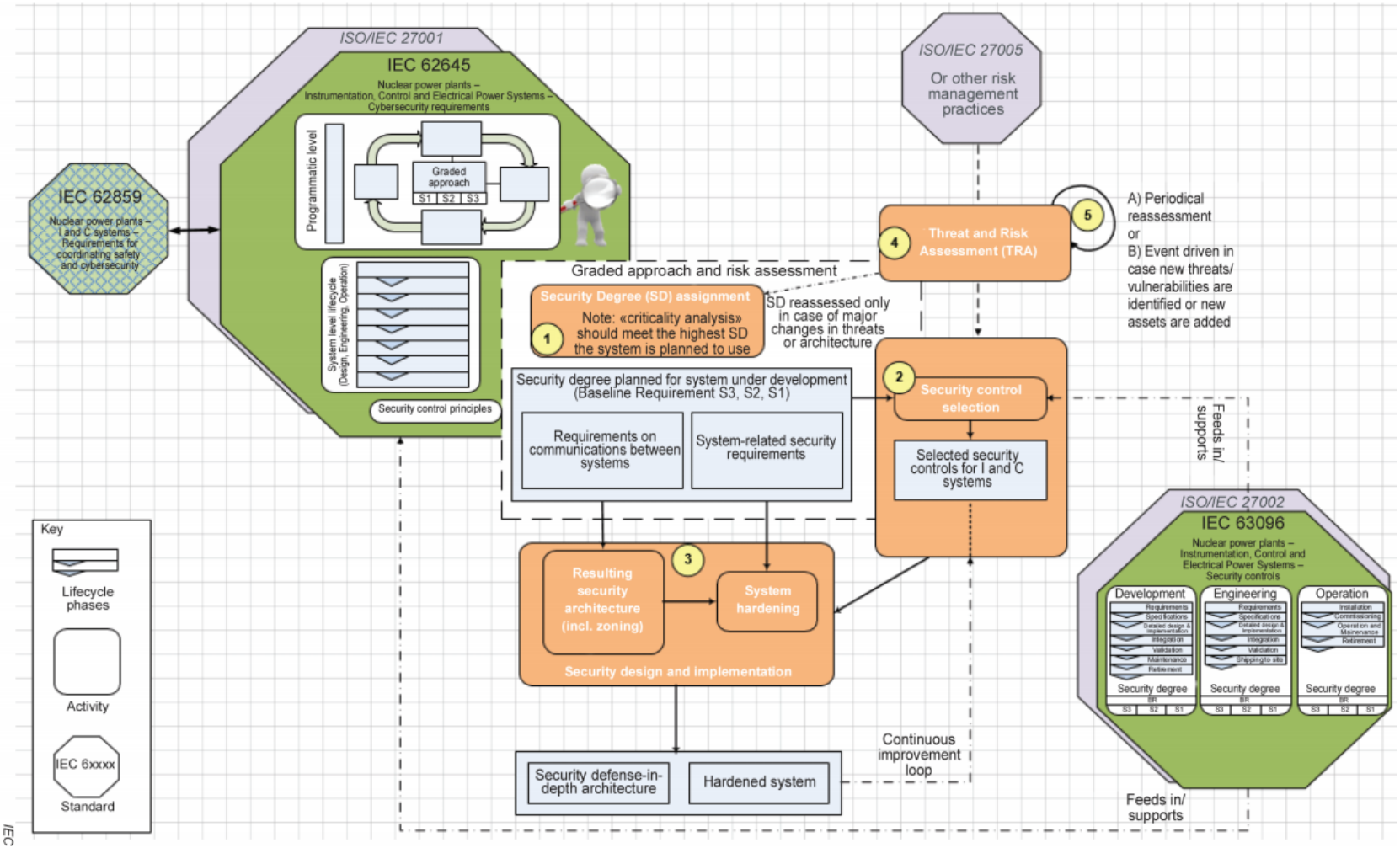
Риск-ориентированный подход

Как сочетается с дифференцированным подходом

Управление рисками охватывает действия по руководству и контролю в отношении рисков

Результаты анализа рисков на уровне станции являются основой для реализации зонирования

Результаты анализа рисков на уровне систем служат технической валидации мер защиты и применению компенсирующих мер


ISO/IEC 27001
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Programmatic level
Graded approach
S1 S2 S3
System level lifecycle (Design, Engineering, Operation)
Security control principles
IEC 62859
Nuclear power plants – I and C systems – Requirements for coordinating safety and cybersecurity
ISO/IEC 27005
Or other risk management practices
4 Threat and Risk Assessment (TRA)
5
A) Periodical reassessment or
B) Event driven in case new threats/ vulnerabilities are identified or new assets are added
Graded approach and risk assessment
Security Degree (SD) assignment
1
Note: «criticality analysis» should meet the highest SD the system is planned to use
SD reassessed only in case of major changes in threats or architecture
Security degree planned for system under development (Baseline Requirement S3, S2, S1)
Requirements on communications between systems
System-related security requirements
2 Security control selection
Selected security controls for I and C systems
Feeds in/ supports
ISO/IEC 27002
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
Development
Engineering
Operation
Security degree
3
Resulting security architecture (incl. zoning)
System hardening
Security design and implementation
Security defense-in-depth architecture
Hardened system
Continuous improvement loop
Feeds in/ supports
Key
Lifecycle phases
Activity
IEC 6xxxx
Standard

Целью является оценка и управление рисками информационной и кибербезопасности, возникающими из потенциальных атак, которые способны в том числе навредить ядерной безопасности или физической ядерной безопасности АЭС

Двухуровневый и двухмодельный подход

- Уровень станции: оценка по функциональной модели (NPP FIC) и на основе ущерба, исходя из потенциального влияния кибератак на функции АЭС
- Уровень систем: оценка по инфраструктурной модели и описанию систем, в том числе исходя из анализа связности систем посредством цифровых интерфейсов

Kaspersky Industrial Cybersecurity Conference

Оценка рисков на уровне АЭС

Как реализована

kaspersky

Оценка рисков на уровне АЭС

1й уровень согласно
МАГАТЭ NSS 17-T

Характеристика АЭС

функции безопасности+
функции нормальной эксплуатации

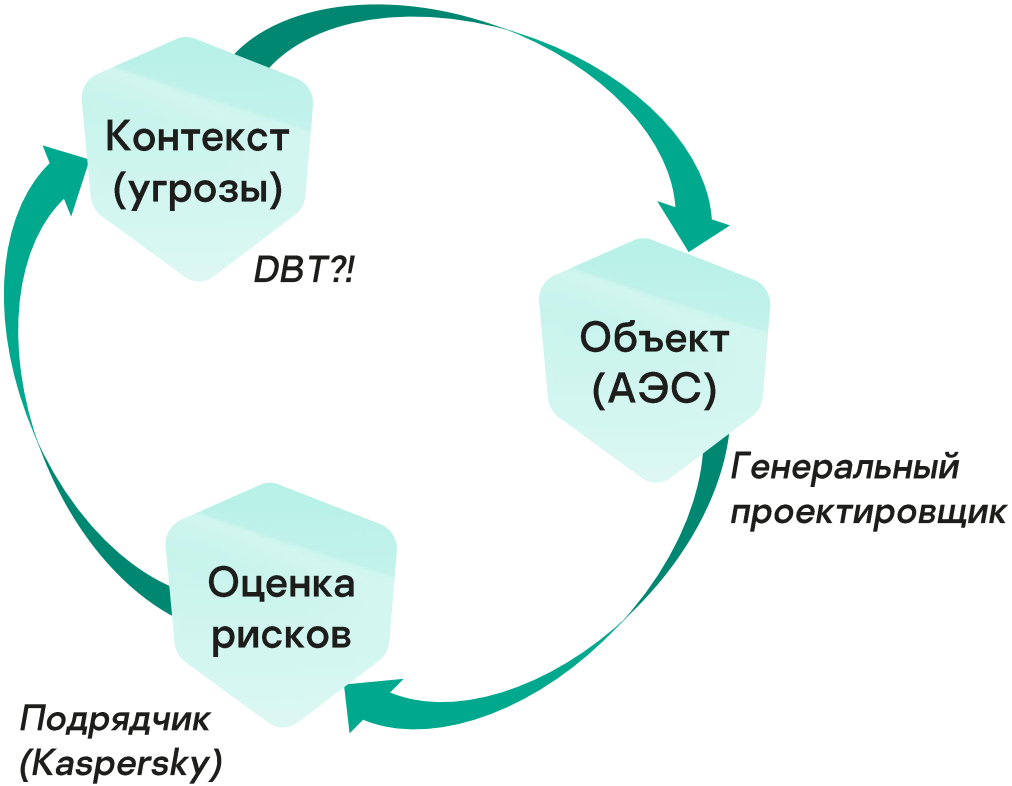
Характеристика угроз

Исследования Kaspersky ICS CERT

Характеристика рисков

Исходя из критериев, представленных в Концепции информационной безопасности

Оценка рисков на уровне АЭС: необходимые сведения и экспертиза



Об объекте
NPP Function Identification and classification

О ландшафте угроз
DBT, Design Basis Threat.

О способе оценки рисков
Risk assessment criteria

Оценка рисков на уровне АЭС: необходимые сведения и экспертиза

Об объекте
NPP Function Identification and classification

О ландшафте угроз
DBT, Design Basis Threat.

О способе оценки рисков
Risk assessment criteria

Оценка рисков на уровне АЭС

Основные моменты

- Консервативная оценка, на основании потенциального отказа функций АЭС
- Критерии оценки наследуются от базовой концепции безопасности, разработанной АЭП и дополненной критериями safety
- Результаты – уровни рисков от Low до Critical для функций безопасности и для нормальной эксплуатации

Kaspersky Industrial Cybersecurity Conference

Оценка рисков на уровне систем

Как реализована

kaspersky

Оценка рисков на уровне систем

2й уровень согласно МАГАТЭ NSS 17-T

Характеристика активов

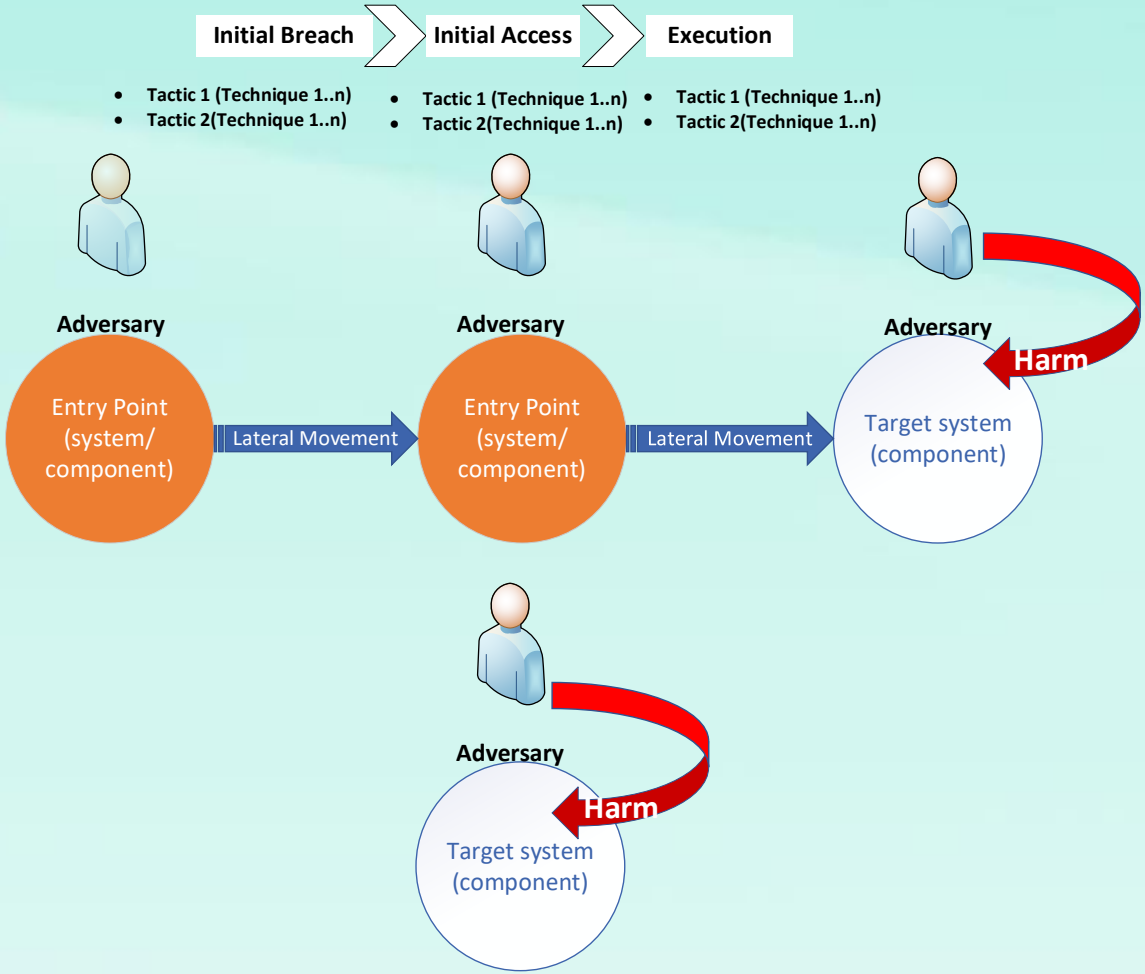
На основе документов Basic Design

Характеристика сценариев атак

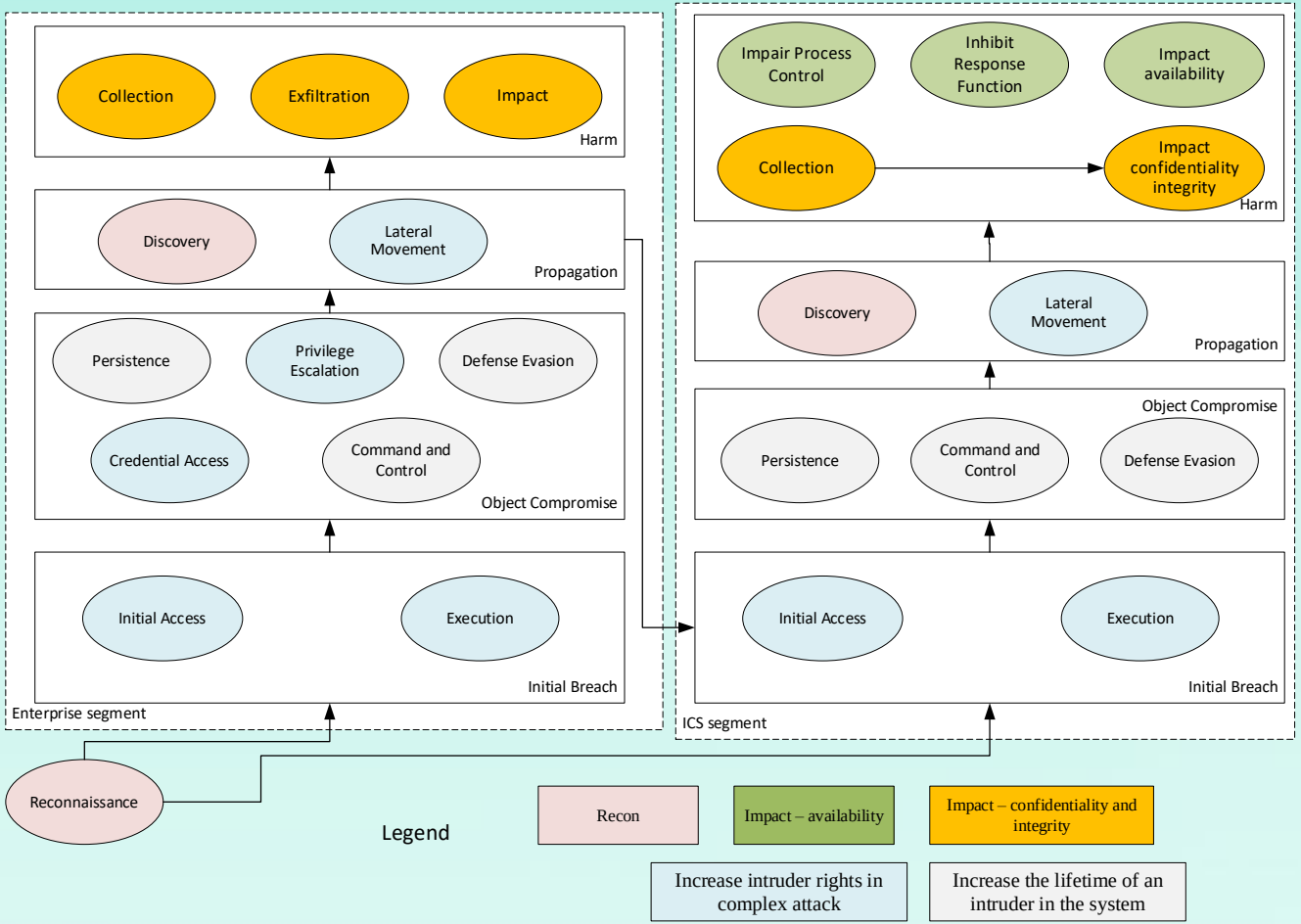
Построение т.н. “killchain” атаки на основе фреймворка MITRE

Характеристика рисков

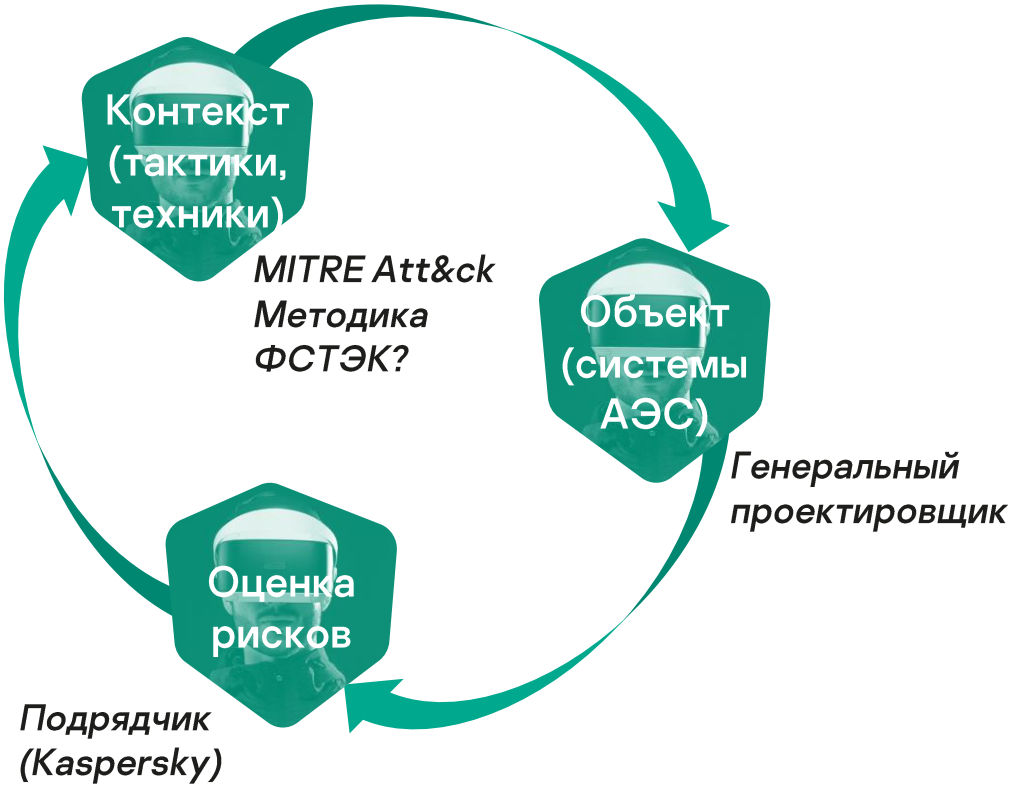
На основе вероятности (likelihood) и тяжести последствий как описано в стандарте ISO 27005


Initial Breach
Initial Access
Execution
Tactic 1 (Technique 1..n)
Tactic 2(Technique 1..n)
Tactic 1 (Technique 1..n)
Tactic 2(Technique 1..n)
Tactic 1 (Technique 1..n)
Tactic 2(Technique 1..n)
Adversary
Entry Point (system/ component)
Lateral Movement
Adversary
Entry Point (system/ component)
Lateral Movement
Adversary
Harm
Target system (component)
Adversary
Harm
Target system (component)

Описание тактики ведения кибератаки (база для сценариев)



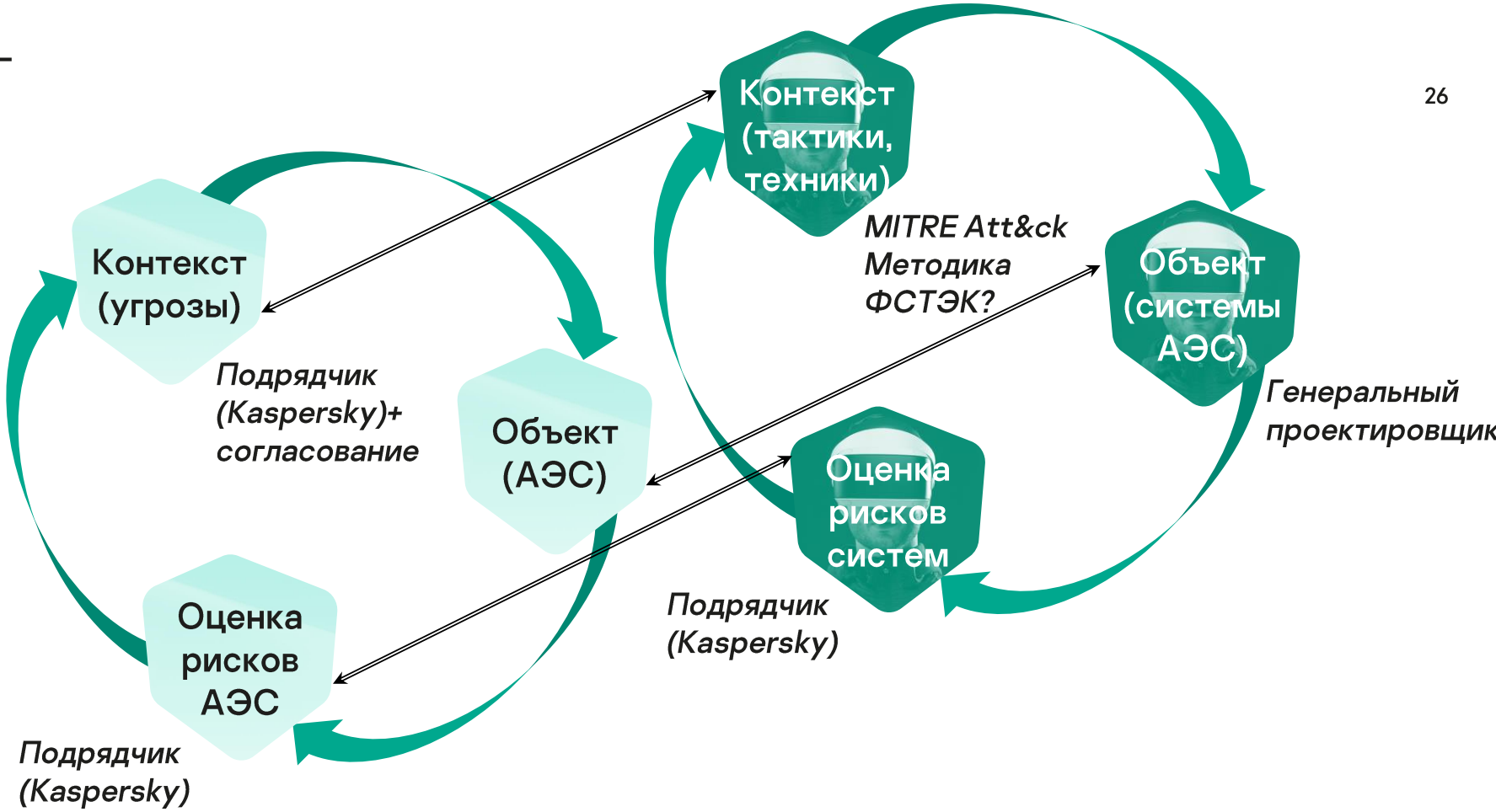
Оценка рисков на уровне систем: необходимые сведения и экспертиза



Об объекте
Basic Design

О тактиках и техниках
MITRE Att&ck
Методика ФСТЭК

О методе оценки рисков
Adversary characteristcs
Threat scenarios
Evaluation method

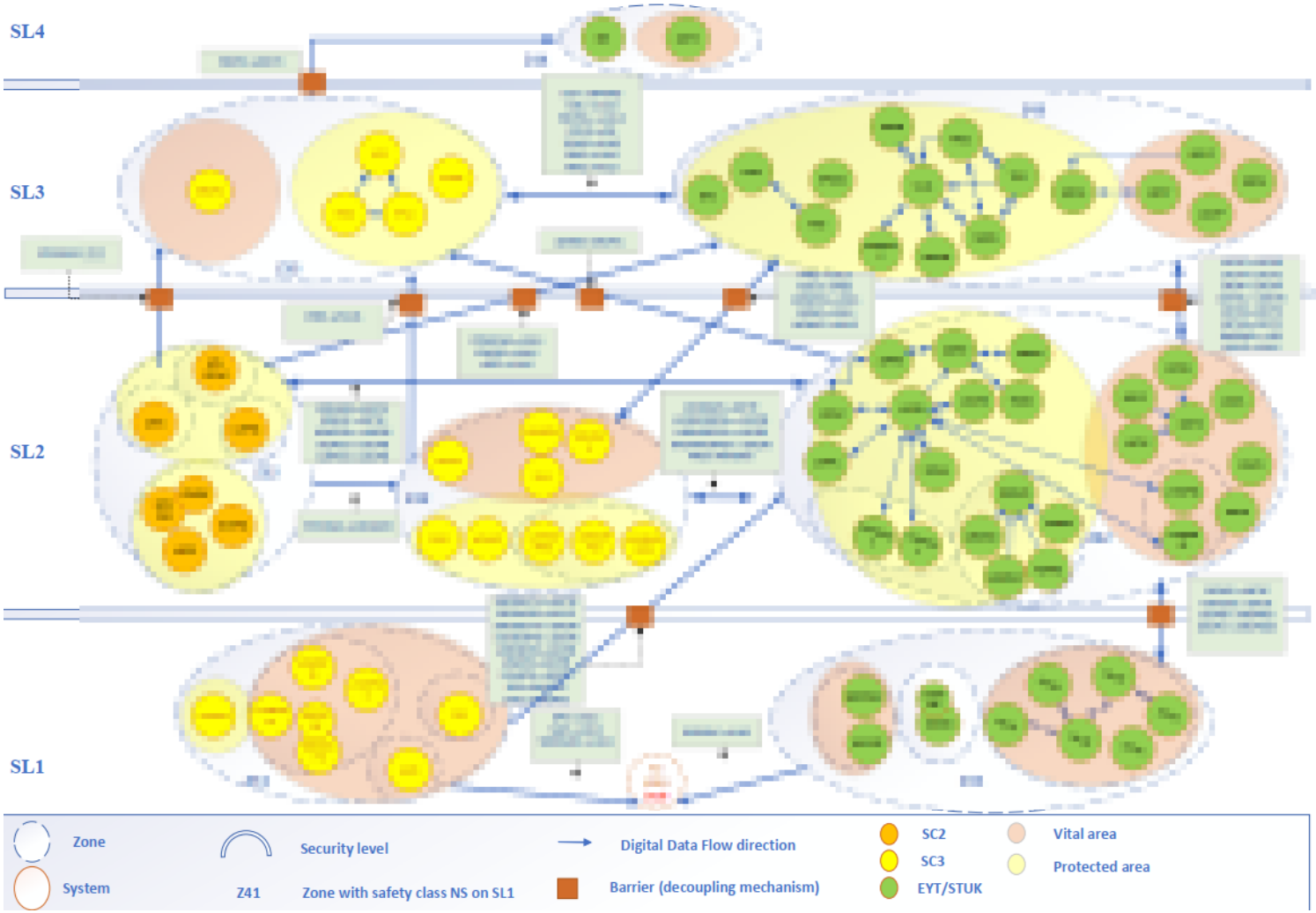

Контекст (угрозы)
Подрядчик (Kaspersky)+ согласование
Объект (АЭС)
Оценка рисков АЭС
Подрядчик (Kaspersky)
Контекст (тактики, техники)
MITRE Att&ck
Методика ФСТЭК?
Объект (системы АЭС)
Генеральный проектировщик
Оценка рисков систем
Подрядчик (Kaspersky)

Kaspersky Industrial Cybersecurity Conference

Результаты

kaspersky

– Выполнена оценка рисков в соответствии с IAEA+ISO+IEC+нац. регулятор, выстроена архитектура кибербезопасности АЭС и валидирована на уровне систем
– (~год работы)


SL4
SL3
SL2
SL1
Zone
System
Security level
Z41
Zone with safety class NS on SL1
Digital Data Flow direction
Barrier (decoupling mechanism)
SC2
SC3
EYT/STUK
Vital area
Protected area

Q

Основные группы документов

Программа информационной безопасности, включая СУИБ и описание ключевых подходов и принципов ИБ

Архитектурный план кибербезопасности АЭС

Методика оценки рисков

Планы оценки рисков

Отчет об оценке рисков уровня АЭС

Отчеты об оценке рисков уровня систем

Планы и спецификации уровня систем

SvetoCopy
CLASSIC
Sylvamo
SvetoCopy
CLASSIC
ДОБРЫЕ ДЕЛА НЕ ТОЛЬКО НА БУМАГЕ

Спасибо за внимание!

Kaspersky ICS CERT

Ekaterina Rudina
Semen Kort
Denis Babaev

https://ics-cert.kaspersky.ru/

kaspersky