Fundamentals of smart grid
information security analysis and assurance
Practicum

E. Brezhnev
Edited by V.S. Kharchenko

Methods and tools of information security assessment of smart grid

Fuzzy methods and tools for information security assessment of smart grid

Process-based approaches for smart grid (I&C) information security assurance

Fundamentals of smart grid information security analysis and assurance. Practicum

Tempus 2013 SEREIN 2016

PRACTICUM

FUNDAMENTALS OF SMART GRID

INFORMATION SECURITY ANALYSIS AND ASSURANCE

2017

Co-funded by the Tempus Programme of the European Union

Министерство образования и науки Украины
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Е.В. Брежнев

Основы анализа и обеспечения информационной безопасности смарт грид

Fundamentals of smart grid information security analysis and assurance

Практикум

Под редакцией В.С. Харченко

Проект

Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR)

2017

УДК 004.9+004.052:621.38
Р13

Викладені матеріали практичної частини начального курсу “Основи аналізу та забезпечення інформаційної безпеки смарт грид” (Fundamentals of smart grid information security analysis and assurance), підготовленого в рамках проекту Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR)

Курс присвячений практиці оцінювання ризиків та інформаційної безпеки смарт грид. Приводиться навчальна програма курсу, опис семінарів, практикумів, методичні рекомендації щодо самостійного вивчення курсу. Даний курс є частиною курсу з “Fundamentals of secure and resilient computing”.

Книга призначена для аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів та засобів оцінювання ризиків, інфомаційної безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Автор:
Є.В. Брежнєв

Рецензенты:
– директор института проблем моделирования в энергетике им. Г.Э. Пухова Национальной Академии наук Украины, доктор технических наук, профессор Мохор Владимир Николаевич;
– директор центра безопасности и обороны (Болгария), PhD, Тодор Тагарев

Є.В.Брежнєв
Р13 **Основы анализа и обеспечения информационной безопасности смарт грид. Практикум** / Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2017. – 128 с.

В пособии изложены материалы практической части учебного курса «Основы анализа и обеспечения информационной безопасности смарт грид» (**Fundamentals** of s**mart grid security analysis and assurance**), подготовленного для аспирантов в рамках проекта Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR). Курс посвящен практике оценивания рисков информационной безопасности смарт грид.

Приводится учебная программа курса, дается описание семинаров, практикумов и тренингов, методические рекомендации по самостоятельному изучению материала курса. Данный курс является частью курса “Fundamentals of secure and resilient computing”.

Книга предназначена для аспирантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, при изучении методов и средств оценивания рисков информационной безопасности смарт грид, а также может быть полезна для преподавателей, ведущих занятия по соответствующим курсам.

Ил. 41. Табл. 26. Библиогр.: 49 назв.

Утверждено на заседании ученого совета Национального аэрокосмического университета имени Н.Е. Жуковского «ХАИ» (протокол № 8 от 18 апреля 2016 г).

УДК 004.9+004.052:621.38

СПИСОК СОКРАЩЕНИЙ

АСУ	Автоматизированная система управления
ИБ	Информационная безопасность
ИУС	Информационно-управляющие системы
ИС	Инструментальное средство
ИТ	Информационные технологии
ИМК	Иерархия матриц критичности
ЛР	Локальные риски
ЛА	Лингвистическая аппроксимация
ЛП	Лингвистическая переменная
ЛЭП	Линии передачи электроэнергии
МИИ	Методах искусственного интеллекта
НКК	Нечеткие когнитивные карты
НМ	Нечеткие множества
ПО	Программное обеспечение
ПБРЭ	План безопасной разработки и эксплуатации
СМК	Система менеджмента качества
ФП	Функция принадлежности
ЭР	Эмерджентные риски

ALE	Annual Loss Expectancy
COBRA	Consultative Objective and Bi-Functional Risk Analysis
CRA	Cyber Risk Analytics
CWW	Computing with Words
FMECA	Failure Mode and Effect Criticality Analysis
ROI	Return on Investment
SMART	Self Monitoring Analysis and Reporting Technology
SCADA	Supervisory Control and Data Acquisition Systems
SC	Soft-computing

ВВЕДЕНИЕ

В пособии изложены материалы практической части учебного курса «Основы анализа и обеспечения информационной безопасности смарт грид» (Founsdamentals of smart grid security analysis and assurance), подготовленного для аспирантов в рамках проекта Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains[1] (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Курс посвящен теоретическим и практическим аспектам анализа и обеспечения информационной безопасности (далее, ИБ) смарт грид систем и их информационно-управляющих систем (ИУС). Данный курс является частью курса “Fundamentals of secure and resilient computing”.

В пособии приводятся описание семинаров, практикумов, тренинга, в приложениях изложены учебная программа курса и методические рекомендации по самостоятельному изучению материалов курса.

В первом разделе приведены материалы семинара по изучению и сравнительному анализу ИС анализа рисков ИБ смарт грид (ИУС). Раздел также содержит описание практикума, направленного на изучение ИС (SecurITree), используемого для анализа ИБ и выбора контрмер снижения рисков систем в смарт грид.

Второй раздел посвящен практическим аспектам оценивания ИБ с использованием нечетких методов, а также обзору ИС, поддерживающих их реализацию. В разделе приведен практикум, направленный на изучение особенностей применения нечеткого

[1] *Этот проект финансируется при поддержке Европейской комиссии. Эта публикация (сообщение) отражает мнения только авторов, и Комиссия не может нести ответственность за любое использование содержащейся в нем информации.*

This project has been funded with support from the European Commission. This publication (communication) reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

расширения матричных методов для оценки рисков кибер инцидентов систем в смарт грид (ИУС) на этапе проектного анализа.

В разделе также представлен практикум по анализу безопасности смарт грид систем и их ИУС с использованием нечеткой логики, реализованной в виде многоуровневой системы нечеткого вывода. Практикум основан на применении ИС Fuzzy Logic Toolbox, позволяющего провести оценку ИБ с использованием экспертных данных. Изложен иллюстративный пример построения многоуровневой системы нечеткого вывода при оценивании ИБ.

Третий раздел содержит материалы семинар по изучению нормативной базы (стандартов), используемых проектными организациями ИУС при выборе решений, направленных на обеспечение (повышение) ИБ ИУС (по требованиям US NRC).

Кроме того, в разделе приведены материалы тренинга, направленного на отработку практических навыков по подготовке плана безопасной эксплуатации и разработки, реализуемого проектными организациями с целью повышения ИБ ИУС критического применения.

Рисунки, таблицы и формулы для удобства нумеруются в пределах каждого раздела.

Книга предназначена для аспирантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, при изучении вопросов информационной безопасности систем смарт грид (ИУС), а также может быть полезна для преподавателей, ведущих занятия по соответствующим курсам.

Пособие подготовлено доцентом кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ» к.т.н., с.н.с. Брежневым Е.В. Общее редактирование проведено проф. д.т.н. Харченко В.С.

Автор выражает благодарность рецензентам, студенту кафедры компьютерных сетей и систем Бородавке В.А. за помощь в подготовке материалов практической части данного курса.

1 МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ ГРИД

1.1 Семинар. Обзор инструментальных средств риск анализа ИБ смарт грид (ИУС)

Цель и задачи семинара:

Целью является обзор инструментальных средств (ИС) риск-анализа ИБ систем смарт грид (ИУС).

Учебные задачи:

– изучение основных положений риск-анализа ИБ смарт грид (ИУС);

– изучение основных ИС риск-анализа ИБ смарт грид (ИУС);

– изучение подходов к проведению риск-анализа смарт грид (ИУС).

Практические задачи:

– проведение аналитического обзора ИС риск-анализа ИБ;

– выполнение учебного проекта по оценке ИС риск-анализа ИБ смарт грид;

– приобретение навыков командной работы при выполнении учебного проекта.

Подготовка к семинару

При подготовке к семинару необходимо:

– уяснить цели и задачи;

–изучить теоретический материал, приведенный в описании, а также в [1-25].

Теоретический материал

Обзор ИС риск анализа ИБ систем смарт грид.

Анализ зарубежных источников подтверждает существование множества ИС для анализа рисков ИБ в смарт грид. По группам они классифицируются на: отраслевые (секторальные), специфические, применимые только в некоторой отрасли, и общие, применимые для многих секторов.

В настоящее время известны следующие ИС анализа рисков ИБ ситсем в смарт грид.

Cyber Risk Analytics (CRA). Cyber Risk Analytics (CRA) предоставляет пользователю базу-данных об угрозах, связанных с нарушением целостности данных или потерей учетных данных, а также рисках ИБ, уязвимостях, специфических для определенной сферы деятцйльности. Это позволяет организациям учесть угрозы, выбрать контрмеры для их снижения в будущем.

Интеграция рейтингов PreBreach в процессы безопасности, а также инструменты управления рисками позволяет организациям избежать дорогостоящих оценок риска, позволяя понять какие риски присутствуют, а также действовать быстро и надёжно для активной защиты своих информационные активов.

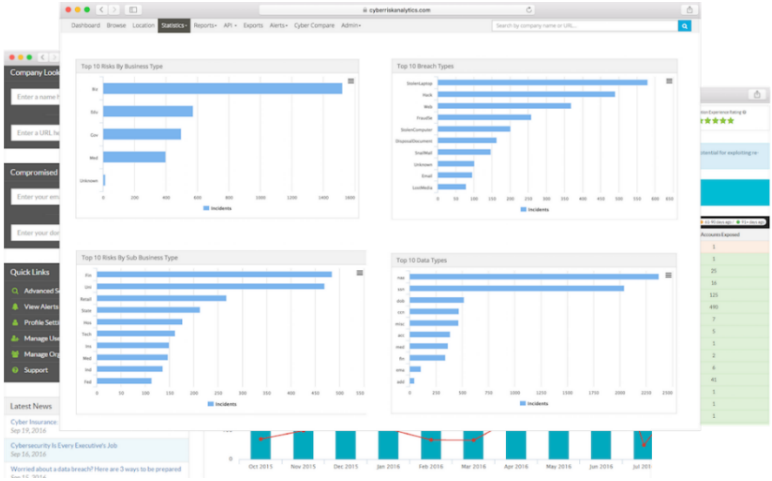


Рисунок 1.1 – Интерфейс Cyber Risk Analytics

RiskWatch. ПО RiskWatch, разрабатываемое американской компанией RiskWatch, Inc., является мощным средством анализа и управления рисками ИБ. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности.

ПО включает в себя следующие средства аудита и анализа рисков:

– RiskWatch for Physical Security –для физических методов защиты ИС;

– RiskWatch for Information Systems – для информационных рисков;

– HIPAA-WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA;

– RiskWatch RW17799 for ISO 17799 – для оценки требованиям стандарта ISO17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются «предсказание годовых потерь» (Annual Loss Expectancy – ALE) и оценка «возврата от инвестиций» (Return on Investment – ROI). Семейство программных продуктов RiskWatch, имеет массу достоинств. К недостаткам данного продукта можно отнести его относительно высокую стоимость.

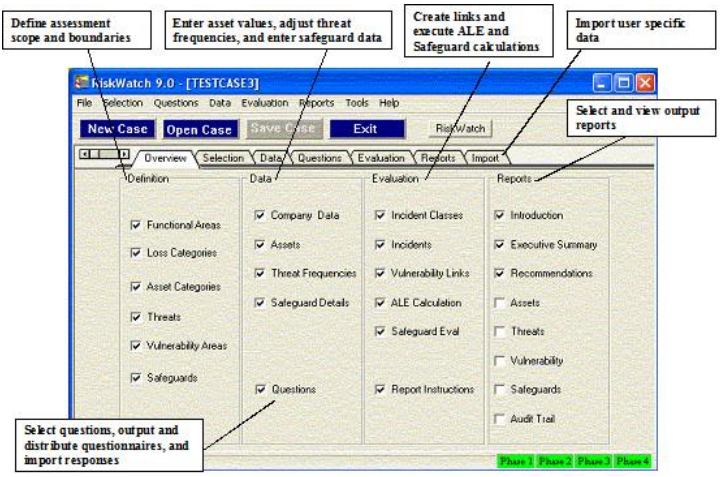


Рисунок 1.2 – Интерфейс RiskWatch

CRAMM. Метод CRAMM (the UK Goverment Risk Analysis and Managment Method) был разработан Службой безопасности Великобритании (UK Security Service) по заданию Британского правительства. Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта, реализующего метод CRAMM.

В настоящее время CRAMM — это универсальный инструмент, позволяющий, помимо анализа рисков ИБ, решать также других аудиторских задач, включая:

- проведение анализа информационных систем и выпуск сопроводительной документации на всех этапах его проведения;
- проведение аудита в соответствии с требованиями Британского правительства, а также стандарта BS 7799:1995 — Code of Practice for Information Security Management BS7799;
- разработку политики ИБ и плана обеспечения непрерывности бизнеса.

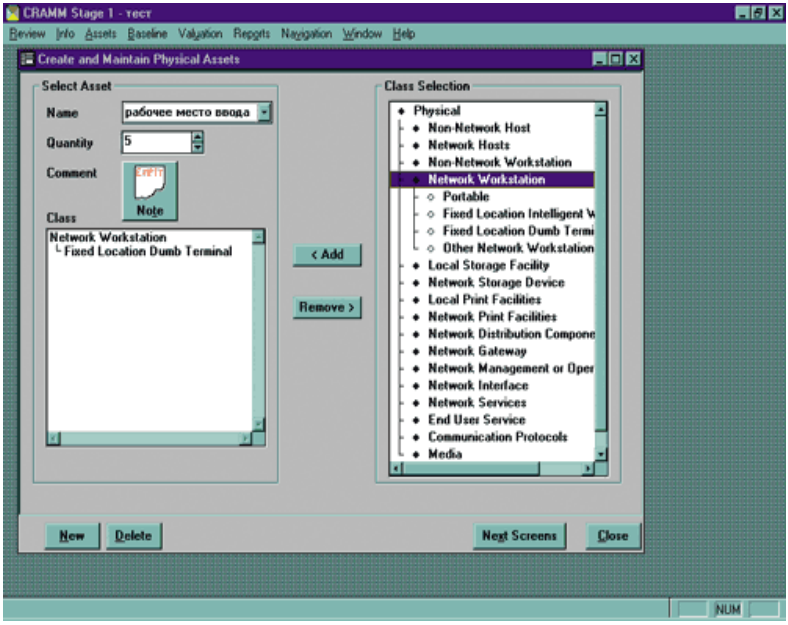


Рисунок 1.3 – Интерфейс CRAMM

ГРИФ. Для проведения полного анализа информационных рисков, прежде всего, необходимо построить полную модель информационной системы с точки зрения ИБ. Для решения этой задачи ПО ГРИФ, в отличие от представленных на рынке западных систем анализа рисков ИБ, обладает простым для пользователя интерфейсом.

ИС реализует сложный алгоритм анализа рисков ИБ, учитывающий более 100 параметров, который позволяет в качестве результат выдать точную оценку существующих в информационной системе рисков, основанную на анализе особенностей практической реализации информационной системы.

Основная задача ПО ГРИФ — дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство компании в необходимости инвестиций в сферу ее информационной безопасности.

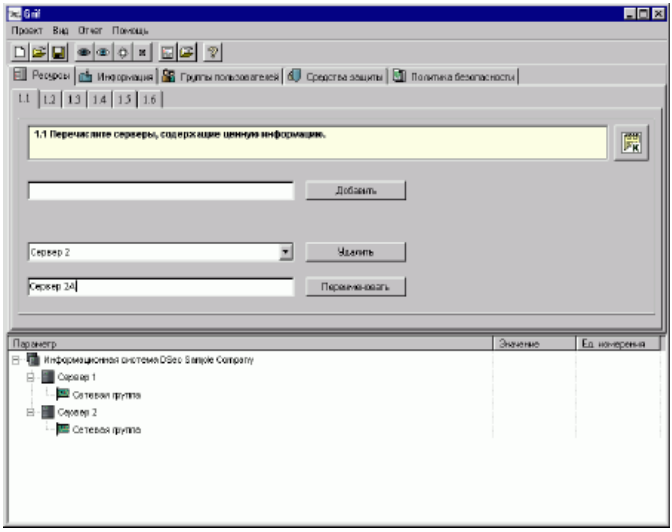


Рисунок 1.4 – Интерфейс ГРИФ

COBRA. Система COBRA (Consultative Objective and Bi-Functional Risk Analysis), разрабатываемая компанией Risk Associates, является средством анализа рисков и оценки соответствия ИС стандарту ISO17799. COBRA реализует методы количественной оценки рисков ИБ, а также инструменты для консалтинга и проведения обзоров безопасности.

При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям, а также большое количество вопросников, с успехом применяющихся на практике. В семейство программных продуктов COBRA входят COBRA ISO17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant.

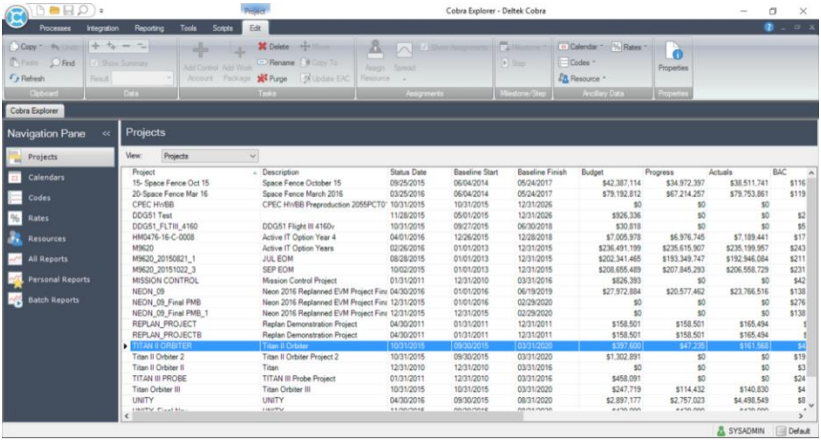


Рисунок 1.5 – Интерфейс COBRA

Buddy System. Программный продукт Buddy System, разрабатываемый компанией Countermeasures Corporation, является еще одним программным продуктом, позволяющим осуществлять как количественный, так и качественный анализ рисков ИБ. Он содержит развитые средства генерации отчетов. Основной акцент при использовании Buddy System делается на информационные риски, связанные с нарушением физической безопасности и управление проектами.

FreeMind. ИС FreeMind предоставляет простой и удобный интерфейс для создания древовидных ассоциативных карт, которые легко могут быть использованы в качестве деревьев атак. Пользователь в программе может определять внешний вид узлов, что позволяет для каждого из специальных типов узлов деревьев атак: И/ИЛИ-декомпозиции, корневого узла, контрмер – задать собственный вид отображения, который затем использовать для всех узлов этого типа.

Программа обладает удобными функциями навигации по такой древовидной структуре, возможности сворачивать, модифицировать и комментировать узлы деревьев.

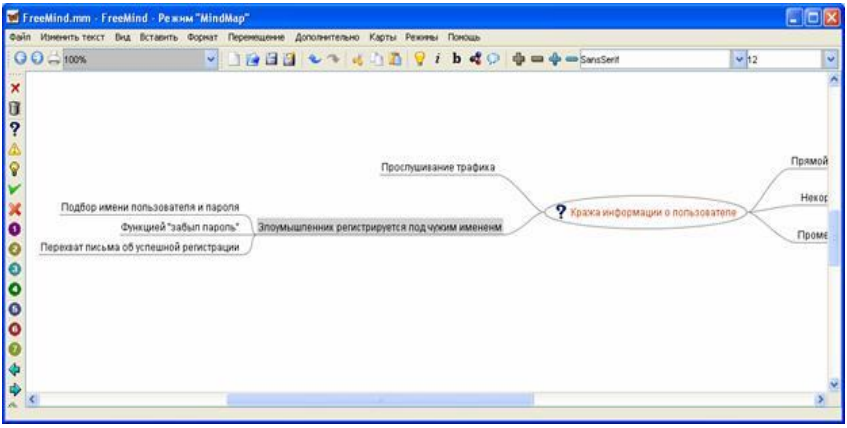


Рисунок 1.6 – Интерфейс FreeMind

SecurITree. SecurITree является ИС для анализа рисков угроз на основе дерева атак. Он работает на базе Windows, Apple и систем Linux.

ИС разработано для работы с деревьями атак, обладает удобным интерфейсом. Продукт хорошо документирован и обладает большим количеством разнообразных специализированных функций, например:

– построение текстовых форм для деревьев;

– построение перечня вариантов реализации атак;

– определение индикаторов атак для расчёта их характеристик (таких как, например, степень опасности того или иного варианта атак);

– возможности создания и использования шаблонов и библиотек атак и т.д.

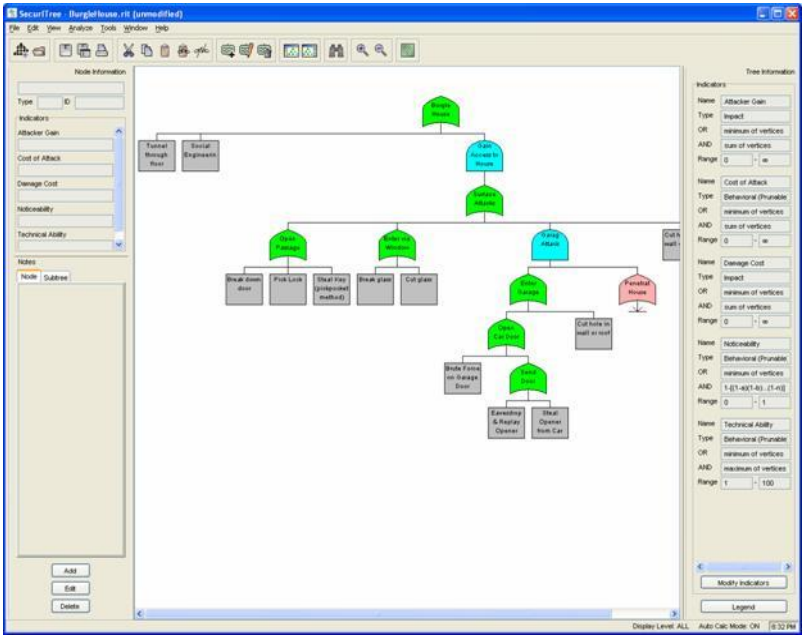


Рисунок 1.7 – Интерфейс SecurITree

Программа разработок и исследований по изучению, сравнительному анализу ИС анализа рисков ИБ смарт грид (ИУС).

Работа выполняется индивидуально и коллективно. Индивидуальная работа предусматривает подготовку каждым студентом презентации по определенному методу оценки безопасности, в соответствии с вариантом (см. таблицу 1.1).

Результатом индивидуальной работы является подготовка и защита презентации.

Презентация разрабатывается в PowerPoint и включает 10-15 слайдов. Время на презентацию – 10 мин.

Презентация должна включать следующие слайды:

- титульный слайд (с указанием ВУЗа, кафедры, дисциплины, темы доклада, автора, даты презентации);
- содержание (структура) доклада;
- перечень функциональных возможностей ИС, перечень задач, решение которых поддерживается;
- основные ограничения и недостатки ИС;
- выводы по докладу;
- список использованных источников.

Каждый из слайдов должен содержать колонтитул с указанием темы и авторов доклада.

Коллективное выполнение работы состоит в организации групповой работы по сравнительному анализу ИС в соответствии с вариантом.

Студенты распределяются на команды. Каждая команда получает задачу, связанную с подготовкой учебного проекта по сравнительной оценке двух ИС анализа ИБ смарт грид.

Варианты заданий приведены в таблице 1.1 (работа в команде).

Этапы создания учебного проекта:

1. Формирование команд. Распределение ролей в команде
2. Выбор группы методов.
3. Постановка целей.
4. Постановка задач.
5. Формирование перечня критериев сравнения ИС.

6. Внутрикомандная работа (дискуссия).

7. Презентация результатов в виде аналитического отчета (требования к содержанию отчета приведены ниже).

После презентации каждой команды, остальные команды должны принимают участие в обсуждении представляемых ИС.

Варианты заданий для подготовки презентаций по ИС анализа ИБ смарт грид приведены в таблице 1.1.

Таблица 1.1 - Варианты заданий для подготовки презентаций по ИС анализа ИБ смарт грид систем

Вариант	Наименование метода риск анализа безопасности
Индивидуальные задания	
1.	Cyber Risk Analytics (CRA)
2.	RiskWatch
3.	CRAMM
4.	ГРИФ
5.	COBRA
6.	Buddy System
7.	FreeMind
8.	SecurITree
Работа в команде	
1.	Комбинации 1,2
2.	Комбинации 1,3
3.	Комбинации 1,4
4.	Комбинации 1,5
5.	Комбинации 1,6
6.	Комбинации 1,8
7.	Комбинации 2,7
8.	Комбинации 3,7
9.	Комбинации 4,7

Требования к содержанию аналитического отчета при выполнении коллективного задания.

Отчет должен содержать:

– титульный лист;

– цели анализа;

– краткое описание ИС, функциональные возможности, перечень решаемых задач;

– преимущества и недостатки данного ИС;

– ограничения по применению;

– результаты сравнительного анализа ИС с указанием критериев сравнения, их оценок для ИС;

– выводы и рекомендации.

Контрольные вопросы

1. Что понимается под смарт грид, каковы основные цели их внедрения?

2. Что понимается под информационной безопасностью смарт грид, основные вызовы и риски смарт технологий?

3. Каковы основные тенденции развития технологий смарт грид?

4. Назовите основные методы риск анализа ИБ смарт грид?

6. Каковы основные отличия ИС, поддерживающих оценку рисков ИБ в смарт грид?

7. Каковы основные практические требования к выбору методов риск анализа безопасности смарт грид и ИУС?

8. Приведите примеры разрабатывающихся проектов смарт грид в Украине?

9. Назовите основные уязвимости современных смарт грид?

1.2 Практикум. Ознакомление с инструментальными средствами анализа рисков ИБ смарт грид. Изучение Secur*IT*ree

Цель и задачи практикума:

Целью практикума является изучение программного пакета для анализа рисков угроз ИБ и выбора контрмер на основе дерева атак Secur*IT*ree.

Учебные задачи:

– изучение основных теоретических сведений об анализе рисков ИБ с использованием дерева атак;

– изучение возможностей и ограничений существующих средств анализа рисков угроз на основе дерева атак (Secur*IT*ree).

Практические задачи:

– получение навыков практического анализа рисков угроз ИБ на основе дерева атак.

Подготовка к практикуму

При подготовке к практикуму необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [39-44];

Теоретический материал. Общая информация ИС Secur*IT*ree

Продукт разработан для работы именно с деревьями атак, обладает удобным интерфейсом, продукт хорошо документирован и обладает большим количеством разнообразных специализированных функций, такими как, например:

– построение текстовых форм для деревьев;

– построение перечня вариантов реализации атак;

– определение индикаторов атак для расчёта их характеристик (таких как, например, степень опасности того или иного варианта атак);

– возможности создания и использования шаблонов и библиотек атак и т.д.

Основные преимущества:

– универсальность — метод подходит практически для любых видов информационных систем;

– гибкость — метод легко модифицировать под свои нужды, создавая свои виды узлов, связей и прочее;

– простота — метод достаточно прост для применения, основные проблемы касаются задачи построения полного и всестороннего обзора проблемы безопасности и защищённости разрабатываемого программного продукта;

– наглядность — как графическая, так и текстовая форма представления деревьев атак обладают большой наглядностью;

– инструментальная поддержка — существует множество различных как специальных, так и универсальных инструментов для работы с такими структурами, как деревья атак.

Рабочий инструмент SecurITree

Для создания нового проекта следует запустить приложение SecurITree, где в пункте меню File -> New Tree или использовать комбинацию клавиш Ctrl+Shift+N (Рис.1.8) и задать имя дерева (Рис.1.9). Для открытия уже готового проекта следует выбрать в пункте меню File -> Open Tree или использовать комбинацию

клавиш Ctrl+O (Рис.1.10). Для сохранения текущего проекта требуется использовать комбинацию клавиш Ctrl+S или выбрать соответствующий пункт в меню File -> Save Tree (Рис.1.11).

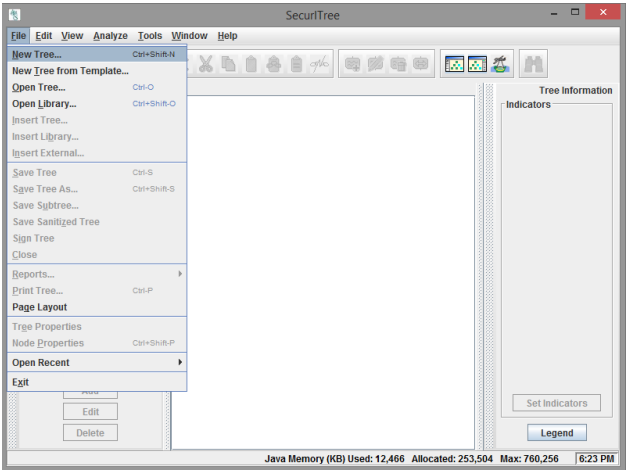


Рисунок 1.8 – Создание нового проекта

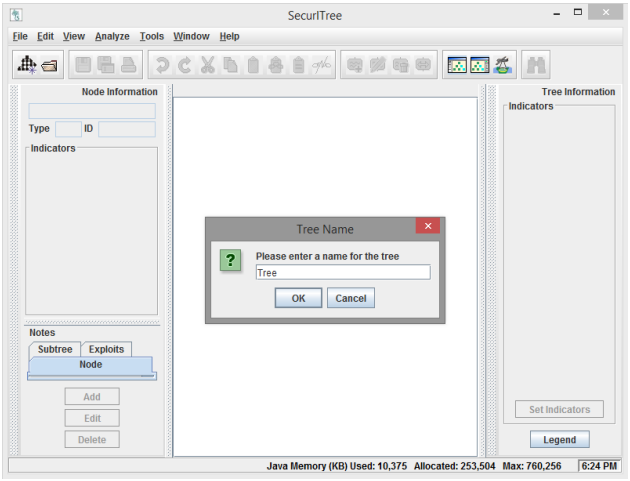


Рисунок 1.9 – Задание имя дерева

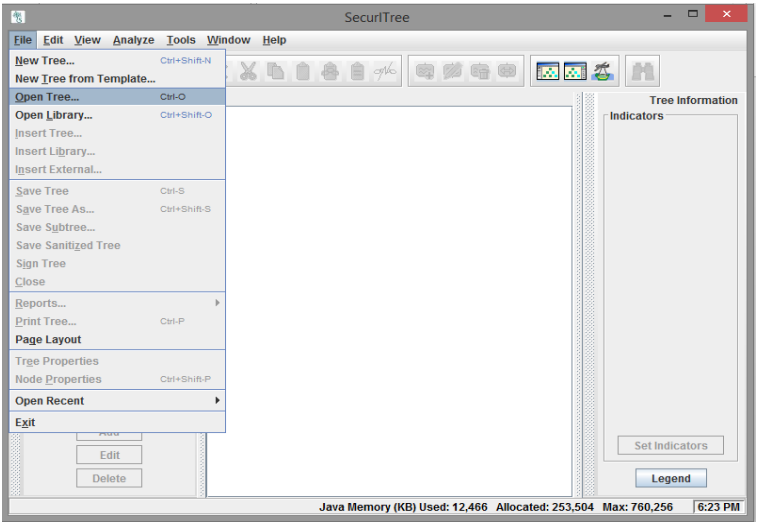


Рисунок 1.10 – Загрузка существующего проекта

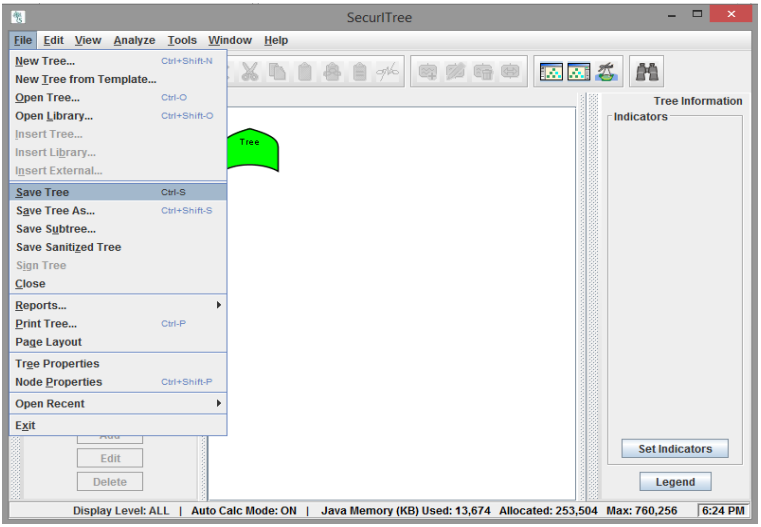


Рисунок 1.11 – Сохранение текущего проекта

Создание дерева атак

Для примера рассмотрим несложную схему нападения на сейф. Каждая схема нападения имеет свою цель, представленную в корневом узле дерева. В нашем примере цель – открытие сейфа. В компьютерных науках деревья «растут» сверху вниз. Чтобы открыть сейф, атакующему нужно открыть замок отмычкой, узнать его шифр, прорезать отверстие в сейфе или сделать что-то при установке сейфа, что позволит потом легко его открыть. Чтобы узнать шифр, взломщик должен либо найти где-нибудь запись комбинации цифр, либо выудить ее у владельца сейфа. И так далее. Каждый узел становится промежуточной целью, а дочерний по отношению к нему узел – это путь ее достижения. Для создания узла необходимо в панели инструментов слева выбрать «Add» и после этого задать настройки узла (Рис. 1.12). Созданный узел представлен на Рис.1.13.

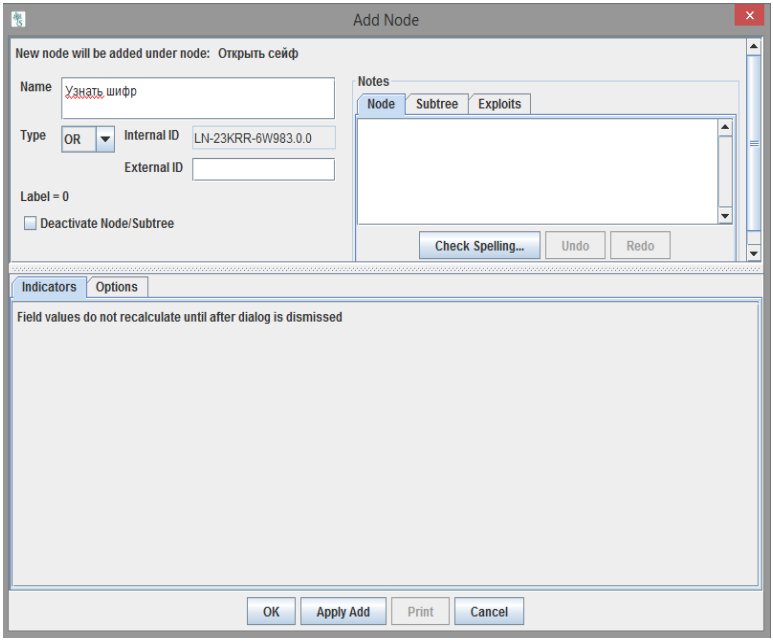


Рисунок 1.12 – Задание настроек узла

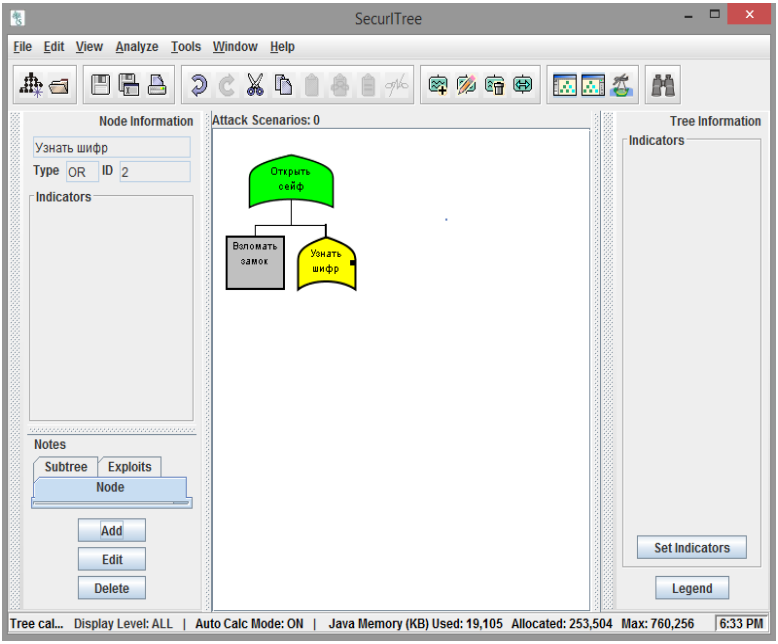


Рисунок 1.13 – Созданный узел

При двойном клике по узлу, который мы создали, открывается окно с его свойствами (Рис. 1.14):

1. В поле «Name», можно задать имя узла схемы;
2. В поле «Type», можно задать тип (Leaf, OR. AND);
3. При нажатии на «Deactivate Node/Subtree» узел деактивируется;

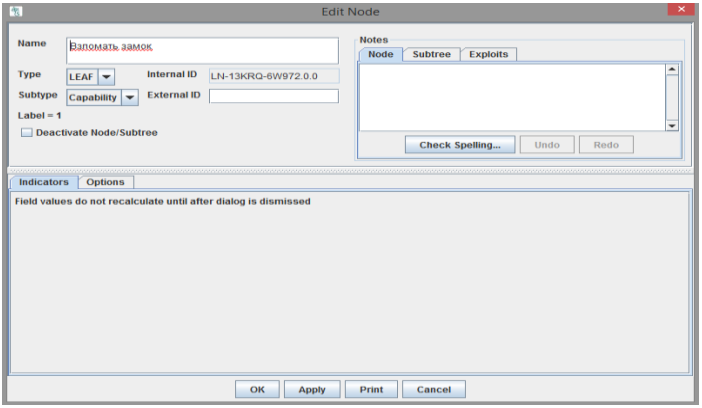


Рисунок 1.14 – Свойства элемента

Согласно примеру, для того, чтобы узнать шифр нужно ИЛИ Найти записанный шифр, ИЛИ Получить шифр у владельца (Рис. 1.15).

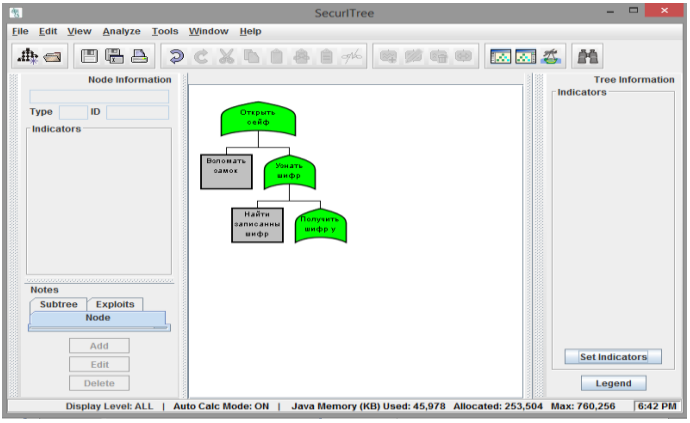


Рисунок 1.15 – Результат добавления узла

В рассматриваемом примере, получить шифр у владельца можно при помощи Угроз, Шантажа, Подкупа ИЛИ Прослушивания (Рис. 1.16), в свою очередь Прослушивание

возможно при *Подслушивании разговора* и *Вынуждении* владельца назвать шифр (Рис. 1.17), в результате чего мы получим дерево атак представленное на рисунке 1.18.

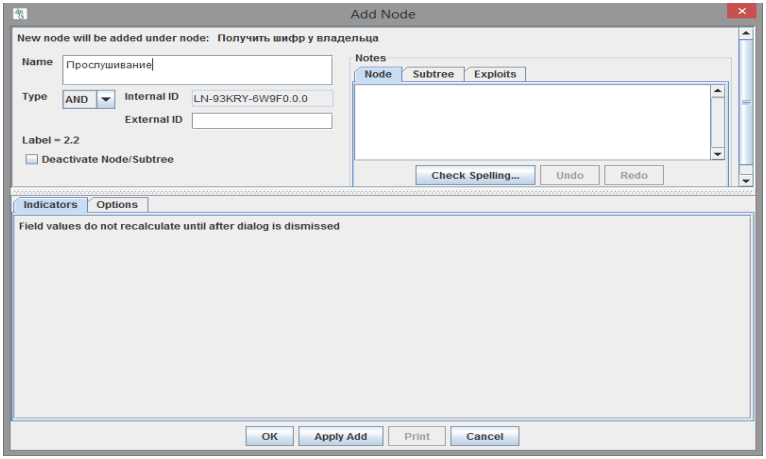


Рисунок 1.16 – Задание настроек узла *Прослушивание*

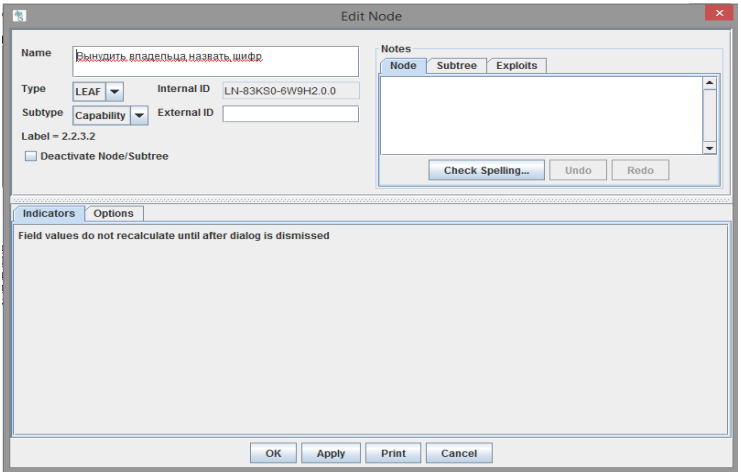


Рисунок 1.17 – Добавление последнего узла

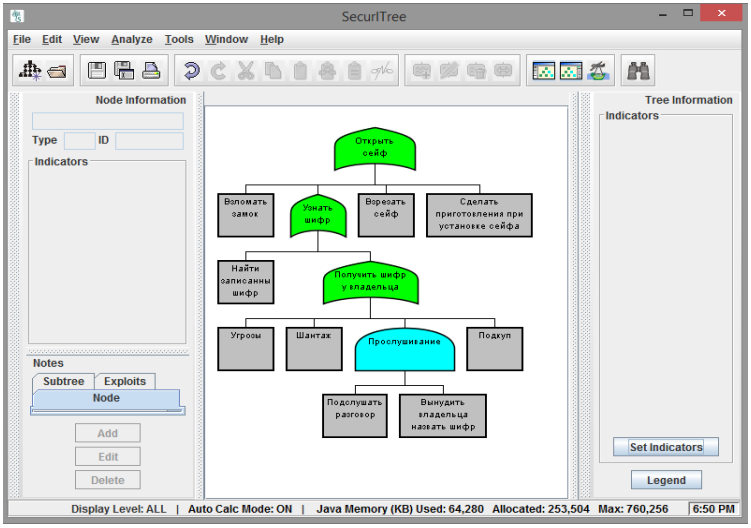


Рисунок 1.18 – Итоговое дерево атак

Для определения сценариев атак необходимо в пункте меню Analyze -> Attack Scenarios (Рис. 1.19).

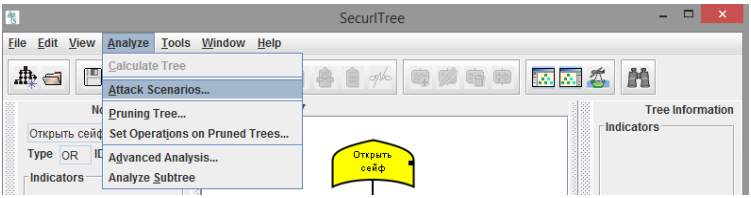


Рисунок 1.19 – Attack Scenarios

Далее на экране появится окно с вариантами возможных атак (Рис. 1.20).

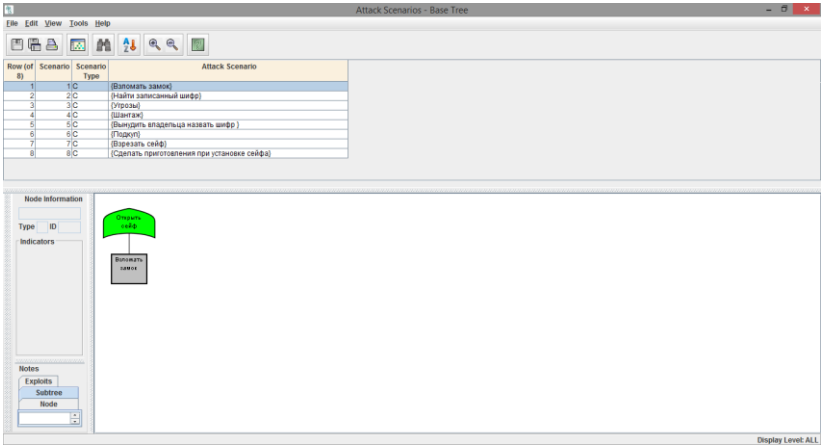


Рисунок 1.20 – Варианты возможных атак

Пример дерева атак на пользовательские данные (Рис. 1.21).

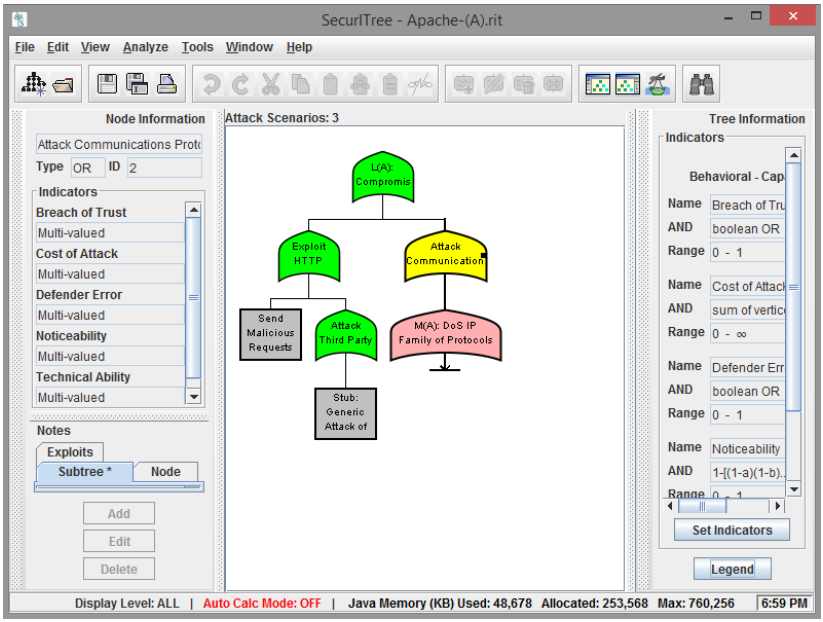


Рисунок 1.21 – Пример дерева атак

Программа разработок

Практикум выполняется индивидуально. Результатом работы является подготовка аналитического отчета.

Аналитический отчет оформляется в виде презентации. Презентация должна включать:

1. Титульный лист.
2. Содержание презентации.
3. Исходные данные описание инцидента в соответствии с вариантом (см. таблицу 1.2).
4. Цепочка событий, приведших к возникновению киберинцидента.
5. Дерево атак для варианта задания.
6. Перечень возможных контрмер для снижения рисков ИБ.
7. Выводы.

Практикум завершается представлением презентации каждым студентом.

Таблица 1.2 - Варианты заданий

№	Наименование объекта	Год	Описание киберинцидента
1.	Russian-Based Dragonfly Group Attacks Energy Industry	2014	Ссылка: http://www.itbusinessedge.com/blogs/data-security/russian-based-dragonfly-group-attacks-energy-industry.html
2.	German Steel Mill Cyber Attack	2014	Ссылка: http://www.risidata.com/Database
4.	Hacker Takes Over Russian Gas System	1999	Ссылка: http://www.risidata.com/Database

Продолжение таблицы 1.2

№	Наименование объекта	Год	Описание киберинцидента
5.	Public utility compromised after brute-force hack attack, says Homeland Security	2014	http://www.navigo.su/index.php?option=com_content&view=article&id=100:2009-10-26-08-37-21&catid=51:2009-09-27-11-41-45&Itemid=86
6.	U-2 spy plane caused widespread shutdown of U.S. flights	2014	http://www.reuters.com/article/us-usa-airport-losangeles-idUSBREA420AF20140503
7.	Iranian Oil Terminal offline after malware attack	2012	http://www.bbc.com/news/technology-17811565
8.	Hackers Attack NZ & Aust for Joining Gulf Taskforce	1998	Ссылка: http://www.risidata.com/Database
9.	DoS Attack Shuts Down Port of Houston	2001	Ссылка: http://www.risidata.com/Database
10.	Slammer Infected Laptop Shuts Down DCS	2003	http://www.risidata.com/Database/Detail/slammer-infected-laptop-shuts-down-dcs
11.	Reverse Osmosis System PLC Attacked	2002	http://www.risidata.com/Database/Detail/reverse-osmosis-system-plc-attacked
12.	Ukraine power grid cyber attack	2015	https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

Контрольные вопросы

1. Перечислите функциональные возможности SecurITree?
2. Назовите основные этапы построения дерева атак?
3. Какой физический смысл узла дерева атак?
4. Что понимается под сценарием атаки?
5. Что понимается под риском информационной безопасности? Назовите основные риски ИБ для смарт грид?
6. Назовите основные ограничения метода анализа дерева атак?
7. Назовите основные контрмеры снижения рисков ИБ в смарт грид?

2 НЕЧЕТКИЕ МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ ГРИД

2.1 Практикум №1. Применение матричных методов для нечеткого оценивания рисков кибер инцидентов систем в смарт грид

Цель и задачи практикума:

Целью является обзор и применение методов оценки рисков ИБ смарт грид на примере нечеткого расширения матричных методов.

Учебные задачи:

– изучение основных положений риск анализа ИБ смарт грид с использованием нечеткого расширения для матричных методов, основ нечеткой математики;

– изучение возможностей и ограничений нечетких методов риск анализа ИБ;

Практические задачи:

– проведение обзора матричных методов оценивания ИБ смарт грид;

– выполнение учебного проекта по анализу ИБ с использованием нечеткого расширения матричных методов;

– приобретение навыков командной работы при выполнении учебного проекта.

Подготовка к практикуму. При подготовке к практикуму необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [26-35].

Теоретический материал

Матричные модели оценивания рисков ИБ являются нечетким расширением FMECA подходов к анализу безопасности. Они позволяют оценить изменение состояний ИБ одних систем смарт грид с учетом наступления киберинцидентов в других системах, связанных с ними.

Под киберинцидентом условимся понимать нарушение нормального функционирования системы, связанного с злоумышленным действием третьих лиц, направленных на изменение (снижение) основных атрибутов ИБ, а именно, целостности, конфиденциальности, доступности.

Состояние ИБ в смарт грид может рассматриваться как состояние отсутствия рисков для основных атрибутов ИБ системы. Состояние ИБ характеризуется уровнем защищенности ИБ активов ИУС от различного рода угроз.

Между состояниями ИБ систем существуют взаимовлияния. Аспект взаимовлияния между состояниями ИБ систем в смарт грид проявляется в случае, когда последствия киберинцидентов одной системы приводят к изменению состояния ИБ другой (зависимой) системы. Взаимовлияние между состояниями ИБ обусловлено наличием информационных связей между системами, т.е. обменом информации между системами в рамках более старшей системы при выполнении функциональных (операционных) задач. Таким образом, для смарт грид информационное влияние между системами является наиболее важным видом взаимовлияния с точки зрения ИБ.

Анализ рисков ИБ состоит в том, чтобы оценить их величину в терминах вероятности киберинцидента и тяжести его последствий, определить меры по их уменьшению и затем убедиться, что риски снижены до приемлемого уровня. Основу процесса составляет определение того, что надо защищать, от кого и как. Для этого выявляются важные системы смарт грид и для каждого из них строится матрица критичности.

Матрица критичности является основным элементом матричных моделей оценивания ИБ. В качестве показателя ИБ для

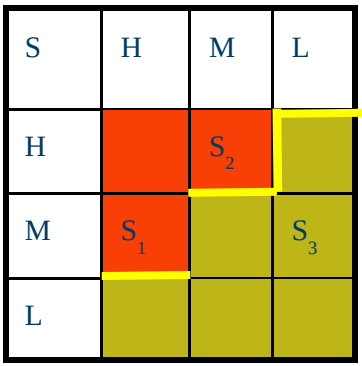
матричных моделей используется *критичность состояния ИБ.*

По смыслу критичность состояния ИБ характеризуется неприемлемыми (с точки зрения спецификации) значениями целостности, конфиденциальности, доступности.

Под матрицей критичности понимается двумерная матрица, описывающая ИБ системы в параметрах вероятности киберинцидента (сбоя) и тяжести (ущерба) его последствий. Матрица критичности позволяет визуализировать состояние ИБ системы. Положение системы в матрице соответствует состоянию безопасности системы.

Матрица критичности имеет вид (см. таблицу 2.1).

Таблица 2.1 – Матрица критичности



Матрица критичности имеет диагональ критичности (выделено желтым цветом), которая позволяет визуализировать требования по ИБ. Нахождение системы над диагональю соответствует не выполнению требований по безопасности (неприемлемые значения ПБ), под диагональю - выполнению требований (приемлемые ПБ).

Исходными данными для построения матрицы критичности является вероятность киберинцидента и тяжесть его последствий. На этапе проектирования систем смарт грид исходные данные могут быть получены на основе анализа исторических данных. Для новых систем, не имеющих аналогов, в качестве источников данных могут выступать эксперты. Для представления субъективных оценок вероятности и тяжести последствий могут

быть использовать лингвистические переменные (ЛП): ВЕРОЯТНОСТЬ И УЩЕРБ.

Каждый терм (значение) ЛП ВЕРОЯТНОСТЬ описывается соответствующей функцией принадлежности (ФП), например, нечетким треугольным числом. Для определения ФП вероятности киберицидента соответствующему лингвистическому терму необходимо определить его вероятность и определить ФП носителя одному из термов значен*ий, используя максимальное значение ФП.*

Так, например, при использовании нечетких треугольных чисел для представления семантики термов (см. рис. 2.1), определение вероятности киберинцидента позволяет определить ФП данного значения множеству нечетких термов по критерию максимума ФП. Это позволяет, используя вероятность киберинцидента системы определить ее положение в одном из строк матрицы критичности.

Вероятность киберицидента может быть получена с использованием метода построения деревьев атак.

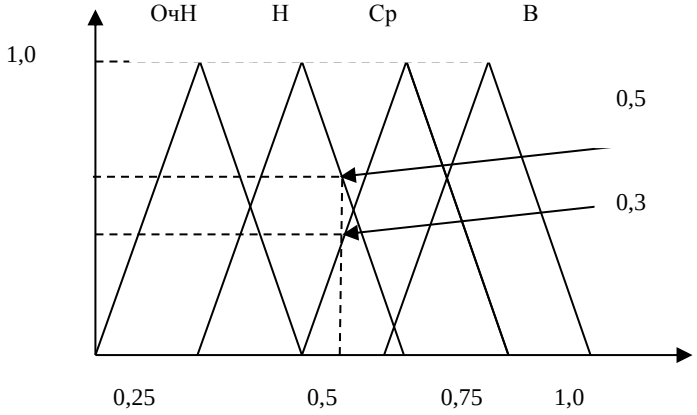


Рисунок 2.1 – ФП ЛП критичности состояния ИБ системы

Аналогично, вводятся ЛП УЩЕРБА, связанного с киберинцидентом (аварией) системы. Задается вид ФП каждого терма и определяется значение функции для каждого носителя ЛП – УЩЕРБ.

При оценке критичности состояния ИБ могут рассматриваться следующие ЛП тяжести последствий аварии системы, приведенные в таблице 2.2.

Таблица 2.2 - ЛП тяжести последствий киберицидента (аварии) системы

№	ЛП	Семантическая интерпретация
1.	*катастрофический кибер инцидент (авария)*	гибель и травмирование людей, значительный ущерб анализируемому объекту, населению, имуществу третьих лиц и окружающей природной среде. Высокие финансовые потери - 1 000 000 $
2.	*критический кибер инцидент (авария)*	угрожает жизни и здоровью людей, наносит существенный ущерб анализируемому объекту, населению, имуществу третьих лиц и окружающей природной среде. Средние финансовые потери - 100 000 $
3.	*некритический киберинцидент (авария)*	не угрожает жизни и здоровью людей, потере объекта, имуществу третьих лиц и окружающей природной среде. Низкие финансовые потери - 1 000 $
4.	киберинцидиент с пренебрежимо малыми последствиями	не относится по своим последствиям ни к одной из первых трех категорий. Очень низкие финансовые потери - 1 00 $

Таким образом, при наличии исторических данных для определения положения системы в матрице критичности необходимо определить:

- вероятность киберинцидента (аварии) системы, используя,

например, статистический или нечеткий подход;

- прогнозируемую величину ущерба, связанную с киберинцидентом (аварией).

Очень важной задачей является построение ФП для каждого терма ЛП. При этом могут быть использованы две группы методов построения функций принадлежности: прямые и косвенные методы.

Прямые методы характеризуются тем, что эксперт непосредственно задает правила определения значений ФП $\mu_A(x)$, характеризующей элемент x.

Косвенные методы построения значений ФП используются в случаях, когда нет элементарных измеримых свойств, через которые определяются нечеткие множества (НМ).

Матрица влияний между состояниями ИБ систем смарт грид.

Информационное влияние $I(t)^{CI}_{inf\,orm}(S_i \to S_j)$ между состояниями ИБ системам может быть описано в виде матрицы влияния, элементами которой являются ЛП величины влияния.

Общий вид матрицы влияния приведен в таблице 2.3.

Таблица 2.3 – Общий вид матрицы влияния $M^{S_i \to S_j}_{inf}$ между состояниями безопасности (для трех систем)

	S_1	S_2	S_3
S_1	-	High	Medium
S_2	-	-	Medium
S_3	High	High	-

Medium (M), High (H) – лингвистические оценки влияния изменения состояния ИБ одной системы на состояние ИБ другой.

Смарт грид может быть описан иерархией матриц критичности (ИМК), соответствующей иерархии самого смарт грид, что позволяет визуализировать состояния и требования по безопасности систем. ИМК не статична, что связано с влиянием факторов безопасности.

Изменение ИМК приведено на рисунке 2.2.

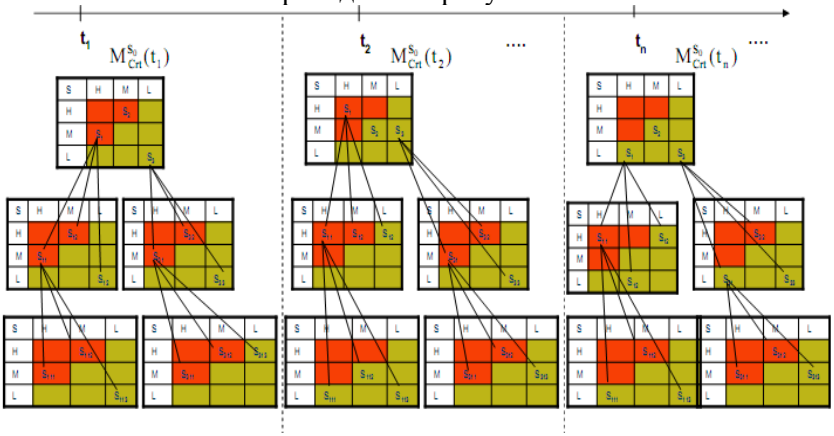


Рисунок 2.2 - Изменение ИМК

ИМК соответствует граф критичности. Графом критичности G_{crt} называется пара $(V(G_{crt}),E(G_{crt}))$, где $V(G_{crt})$ - непустое конечное множество элементов, называемых вершинами графа критичности (матрицы критичности), а $E(G_{crt})$ - конечное семейство неупорядоченных пар элементов из $V(G_{crt})$ (необязательно различных), называемых ребрами (по типам взаимовлияния между системами смарт грид).

В матрице критичности множество киберинцидентов (аварий) разбивается на два подмножества. Подмножество киберинцидентов подсистем, расположенных над диагональю матрицы критичности $M_{inf}^{S_i \to S_j}$ (множество критичных киберинцидентов), и подмножество киберинцидентов, расположенных под диагональю матрицы $M_{inf}^{S_i \to S_j}$ (множество некритичных киберинцидентов).

Этапы метода оценивания ИБ с использованием иерархии матриц критичности.

Этапы метода оценивания ИБ с использованием ИМК приведены на рисунке 2.3.

1.Этап проектного анализа ИБ в смарт грид. Построение

матриц критичности компонентов, подсистем, систем.

На этапе проектного анализа ИБ построение ИМК смарт грид S_0 проводится с целью проверки достаточности, эффективности и контроля решений, направленных на совершенствование оборудования и технологий, обеспечивающих предупреждение или ослабление критичности киберинцидентов, достижение требуемых характеристик ИБ, эффективности и надежности.

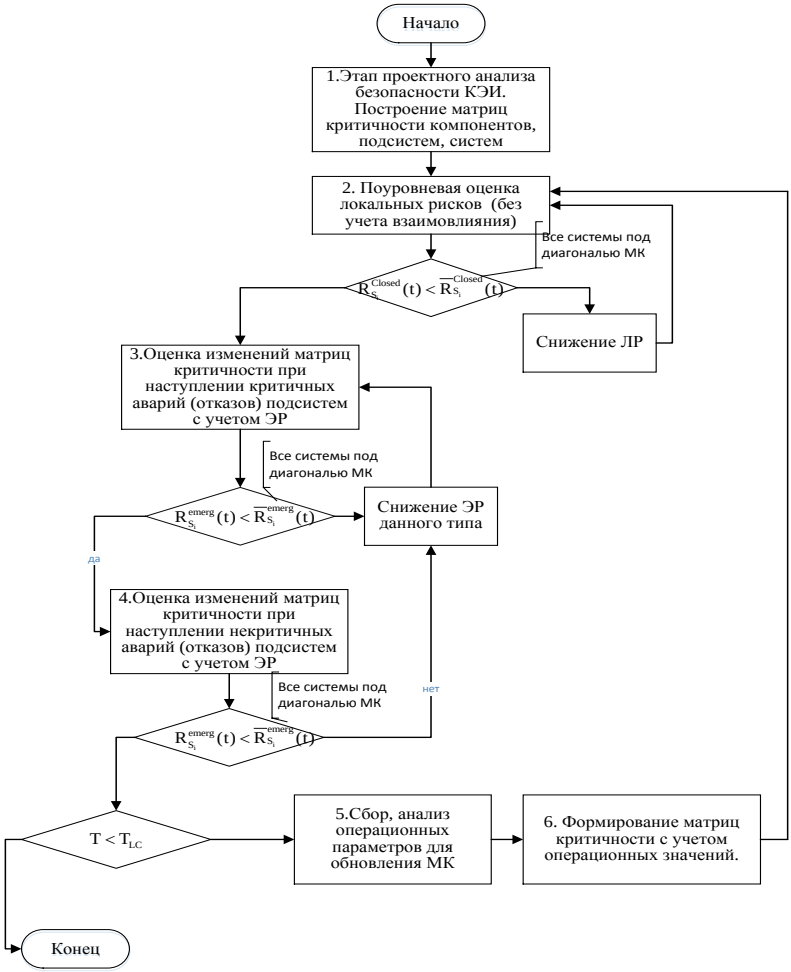


Рисунок 2.3 – Этапы метода оценивания ИБ смарт грид систем с использованием ИМК

Входными данными для построения проектной матрицы критичности являются: спецификации систем (подсистем, компонентов) смарт грид; статистика киберинцидентов с характеристиками частоты проявления и тяжести последствий для систем смарт грид, имеющих аналоги; субъективные оценки показателей критичности (вероятности и тяжести) для уникальных систем, полученные от экспертов; матрица взаимовлияния $M_{inf}^{S_i \to S_j}$, характеризующая влияние информационного типа; экспертные оценки о тяжести последствий киберинцидентов (аварий) систем, подсистем, смарт грид в целом.

Пример проектной ИМК систем смарт грид (без учета взаимовлияния) представлен на рисунке 2.4.

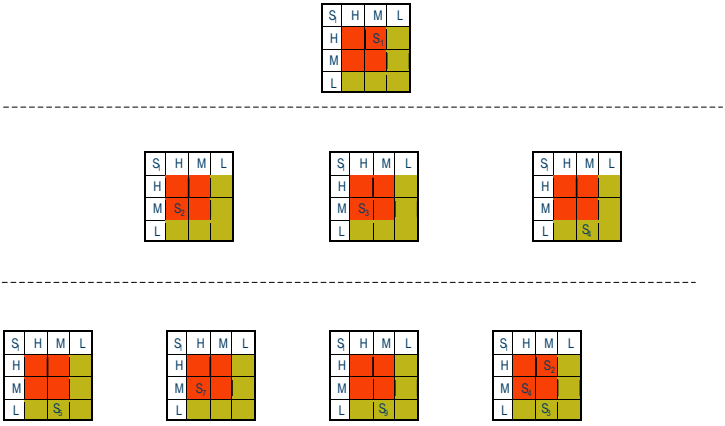


Рисунок 2.4 - Пример проектной иерархии матриц критичности систем смарт грид

2. Поуровневая оценка локальных рисков ИБ (без учета взаимовлияния). Для каждой системы, подсистемы, пр. проводится оценка критичности состояния ИБ. Если система находится над диагональю критичности проводятся контрмеры для снижения ЛР

и повышения безопасности.

3. Оценки изменений матриц критичности при наступлении критичных отказов с учетом взаимовлияния.

Входными данными этапа является: граф критичности; матрицы взаимовлияния $M_{inf}^{S_i \to S_j}$, характеризующие информационное влияние; требуемые уровни ЛР для каждой системы.

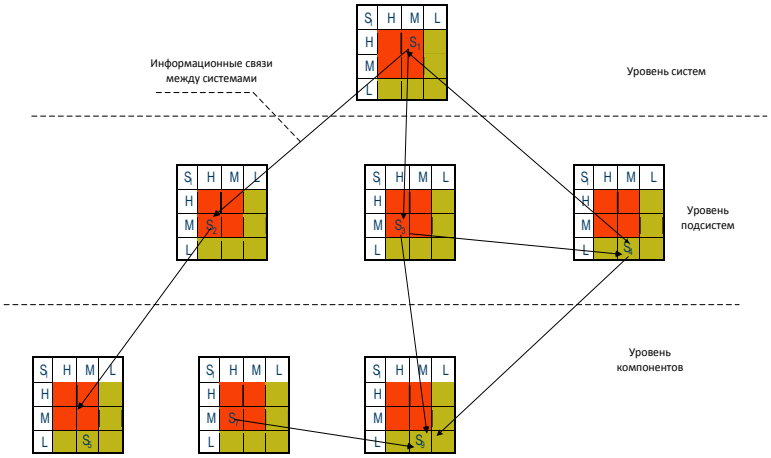


Рисунок 2.5 - Граф критичности систем в смарт грид

Обновление матриц критичности проводится с использованием лингвистической аппроксимации (ЛА). С учетом результатов моделирования формируется новый граф критичности, обновленный с учетом оценивания последствий киберинцидента оной системы и всех систем, связанных с ней. Далее, проводится анализ результатов, оценка выполнения требований по безопасности и реализуется стратегия менеджмента рисками ИБ.

Кратко изложим идею использования ЛА.

Для моделирования ИБ с целью обновления оценок критичности состояния ИБ, предлагается использовать лингвистическое моделирование безопасности, основанное на

адаптации и развитии алгоритма нечетких когнитивных карт (НКК). Методология НКК является символическим представлением для описания и моделирования сложных систем. НКК описывают различные аспекты поведения сложных систем в терминах концепций. Каждая концепция представляет собой состояние или характеристику сложной системы. Эти концепции взаимодействуют между собой.

В рамках данного подхода, концепции - это состояние ИБ, отношения - величина негативного взаимовлияния между состояниями. Особенность подхода в том, что концепции и веса описаны как ЛП. В рамках данной работы алгоритм НКК дополнен аспектом лингвистического моделирования безопасности.

Лингвистическое моделирование безопасности предполагает процесс CWW (Computing With Words). Существует две классические лингвистические вычислительные модели, которые обеспечивают лингвистические операторы для CWW. Это семантическая модель, основанная на принципе расширения и символическая модель.

Рассмотрим подход для получения новых оценок критичности, основанный на использовании семантической модели с принципом расширения.

Принцип расширения используется для обобщения четкой (обычной) математики для нечетких множеств (НМ). Однако его использование увеличивает нечеткость результатов. Результаты, полученные с помощью нечеткой арифметики, являются нечеткими множествами, которые обычно не совпадают ни с одним из первоначальных термов. Для представления новых оценок критичности в области исходных термов проводится лингвистическая аппроксимация.

Оценка критичности представляется в виде ЛП, которая характеризуется:

- синтаксическим правилом в форме грамматики, порождающей название значений переменной;
- семантическим правилом М, определяющим алгоритмическую процедуру для вычисления смысла каждого значения.

Для представления семантики лингвистических термов

оценок критичности предлагается использовать нечеткие числа с треугольной ФП. Под нечеткой оценкой критичности Crt(S), (представленной треугольным числом L_i) понимается тройка $<a_i, b_i, c_i>$ ($a_i \le b_i \le c_i$) действительных чисел, через которые его функция принадлежности $\mu_{L_i}(x)$ определяется следующим образом:

$$\mu_{L_i}(x) = \begin{cases} \dfrac{x - a_i}{b_i - a_i}, \text{ если } x \in [a_i, c_i], \\ \dfrac{x - c_i}{b_i - c_i}, \text{ если } x \in [b_i, c_i], \\ 0, \text{ в противном случае.} \end{cases} \quad (2.1)$$

Семантика лингвистических оценок в матрице влияния между состояниями также представляется нечетким треугольным числом $P_i <e_i, r_i, m_i>$.

На рисунке 2.6 представлена семантика семи термов критичности, $S = \{S_0{:}N, S_1{:}VL, S_2{:}L, S_3{:}M, S_4{:}H, S_5{:}VH, S_6{:}P\}$, с функциями принадлежностей вида:

$$\mu_H = (0.5, 0, 67, 0.83); \mu_{VH} = (0.67, 0.83, 1);$$
$$\mu_P = (0.83, 1, 1); \mu_{VL} = (0, 0.17, 0.33);$$
$$\mu_L = (0.17, 0.33, 0.5); \mu_M = (0.33, 0.5, 0.67);$$
$$\mu_N = (0, 0, 0.17).$$

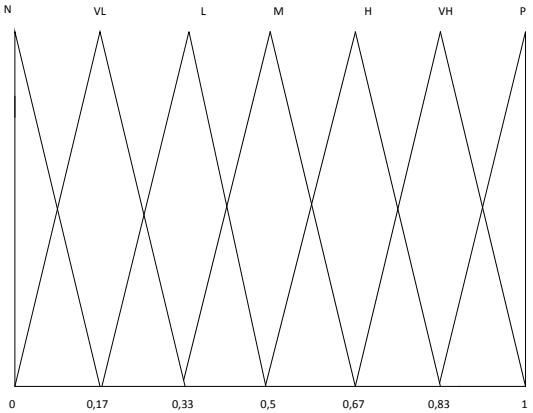


Рисунок 2.6 - ФП лингвистических термов

Множество лингвистических термов должно удовлетворять требованиям:

- существования оператора отрицания Neg (L_i)=L_j, такого, чтобы *j=g-i (g+1-* кардинальность);

- существования оператора минимума и максимума, $L_i \le L_j \Leftrightarrow i \le j$.

Оператор лингвистической агрегации, основанный на принципе расширения, может быть представлен как:

$$\mathbf{L}^n \xrightarrow{\tilde{F}} \mathbf{F(R)} \xrightarrow{app_1(\cdot)} \mathbf{L} \qquad (2.2)$$

где L^n - декартово произведение лингвистических термов;

$\tilde{F}$ - оператор агрегации, основанный на принципе расширения;

$F(R)$ - набор НМ на множестве вещественных чисел R;

$app_1 : F(R) \to L$ - функция лингвистической аппроксимации, определяющая НМ (из исходного набора НМ), ближайшее к полученному НМ;

L – первоначальное множество термов.

Если происходит кибер инцидент (отказ) в системе смарт грид, то матрица критичности, содержащая новые оценки критичности, может быть получена путем мультипликации двух нечетких треугольных чисел, описывающих семантику оценок начальной критичности состояния ИБ и негативного влияния между системами.

Другими словами, если S и P нечеткие треугольные числа, то согласно принципу обобщения Заде, новая оценка критичности - нечеткое треугольное число $C = (a_j, b_j, c_j)$ - также является треугольным и характеризуется тройкой <a_j, b_j, c_j>, где

$$a_j = \min \{a_i*e_i, a_i*m_i, c_i*m_i\};$$
$$c_j = \max \{a_i*e_i, a_i*m_i, c_i*e_i, c_i*m_i\};$$
$$b_j = b_i*r_i.$$

Эта оценка не совпадает с первоначальными термами исходного множества лингвистических оценок критичности S_i.

Для представления полученных результатов в первоначальных термах, применяется лингвистическая аппроксимация, основанная на оценке Евклидова расстояния вида:

$$d(L_i, C_j) = \sqrt{P_1(a_i - a_j)^2 + P_2(b_i - b_j)^2 + P_3(c_i - c_j)^2}, \quad (2.3)$$

где (a_i, b_i, c_i) – параметры ФП первоначального лингвистического терма L_i;

(a_j, b_j, c_j) – ФП полученного НМ, характеризующего семантику новой лингвистической оценки критичности отказа;

p_1, p_2, p_3 – веса, характеризующие репрезентативность параметров a, b, c, которые удовлетворяют требованиям вида:

$$P_i \in [0,1]; \sum_i P_i = 1. \quad (2.4)$$

Функция $app_1(\bullet)$ определяет лингвистический терм L_1^*, $app_1(C_j) = L_1^*$, для которого выполняется условие, $d(L_1^*, C_j) \le d(L_1^*, C_j)\ \forall L_1 \in L$.

На рисунке 2.7 приведена графическая иллюстрация семантического подхода, основанного на принципе расширения Заде.

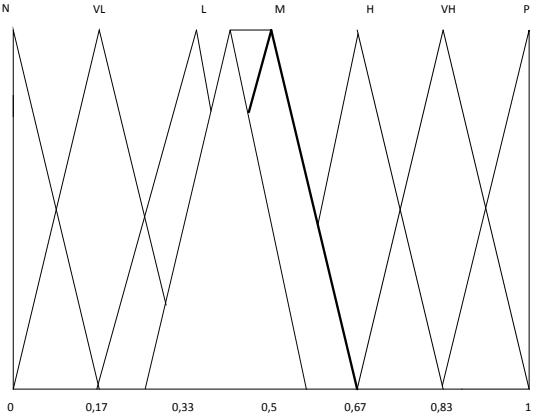


Рисунок 2.7 - Иллюстрация семантического подхода, основанного на принципе расширения Заде

Штриховой линией показано новое треугольное число, которое не совпадает ни с одним из приведенных нечетких треугольных чисел. С использованием оператора ЛА для полученной нечеткой оценки определяется ближайшая нечеткая оценка критичности из исходного множества.

Процедура для определения новой матрицы критичности с учетом отказов систем и информации, характеризующей влияние отказов на критичность отказов других систем, графически представлена на рисунке 2.8.

Таким образом, ИМК применяются в условиях ограниченной статистической информации на всех этапах ЖЦ смарт грид, для анализа локальных и эмерджентных рисков. В основе подхода лежит лингвистическая вычислительная модель с использованием функций принадлежности.

Применение ИМК позволяет использовать информацию, представленную экспертами в виде выражений естественного языка.

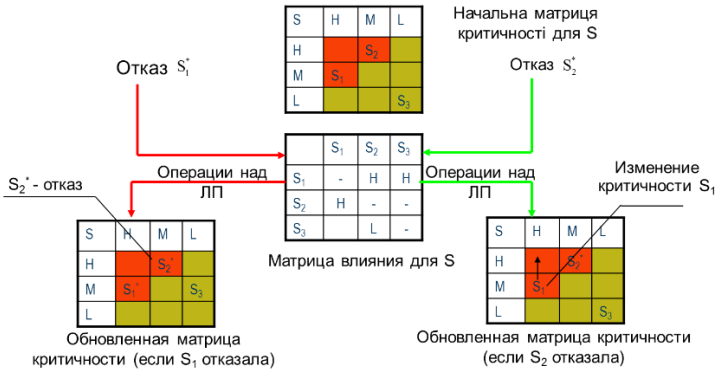


Рисунок 2.8 - Процедура определения новой матрицы критичности с учетом влияния отказов систем

Применение нечеткой математики позволяет оперировать с нечеткими множествами, представляющими семантику нечетких оценок критичности. CWW процедура, использующая оценки влияния отказов, представленных в матрице влияния, позволяет получать прогнозные оценки критичности отказов и учитывать зависимость между отказами.

4. *Оценка изменений матриц критичности при наступлении некритичных киберинцидентов подсистем.*

Некритичный киберинцидент любой подсистемы может инициировать наступление критичных киберинцидентов при условии наличия зависимостей между ними. Сценарии изменения критичности инцидентов определяются видом матрицы влияния. Оценки влияния некритичных кибер инцидентов на критичные инциденты, представленные в виде матриц влияния $M_{inf}^{S_i \to S_j}$, являются дополнительной характеристикой данных инцидентов и могут быть использованы для определения приоритетности мероприятий по снижению ЛР и ЭР в смарт грид.

Входные данные: граф критичности; матрицы взаимовлияния $M_{inf}^{S_i \to S_j}$, характеризующие информационное влияние; требуемые уровни рисков ИБ для каждой системы.

Для обновления матриц критичности используется ЛА. Далее,

проводится анализ результатов, оценка выполнения требований по безопасности и реализуется стратегия менеджмента ЭР.

5.После ввода систем смарт грид в эксплуатацию проводится обновление информации для построения ИМК, соответствующих текущему этапу ЖЦ. Для этого проводится сбор и анализ операционных параметров систем (см. выше).

6. Формирование ИМК с учетом операционных значений. Далее, все вышеуказанные этапы повторяются для обновленных матриц критичности.

Таким образом, обновление ИМК проводится путем моделирования киберинцидентов (аварий) активов любого уровня и оценивании его последствий для систем (подсистем, компонентов) в смарт грид.

Поскольку этап проектного анализа характеризуется высоким уровнем неопределенности, то проектные критичности систем могут существенно отличаться от операционных значений.

Таким образом, ИМК применяются в условиях ограниченной статистической информации на всех этапах ЖЦ смарт грид, для анализа локальных и эмерджентных рисков. В основе подхода лежит лингвистическая вычислительная модель с использованием функций принадлежности.

Применение ИМК позволяет использовать информацию, представленную экспертами в виде выражений естественного языка.

Применение нечеткой математики позволяет оперировать с нечеткими множествами, представляющими семантику нечетких оценок критичности. CWW процедура, использующая оценки влияния отказов, представленных в матрице влияния, позволяет получать прогнозные оценки критичности отказов и учитывать зависимость между отказами.

Программа разработок и исследований

Работа выполняется в два этапа:

1. Разработка программы (ИС) для реализации матричного метода оценивания ИБ в соответствии со спецификацией.
2. Анализ кибер инцидента с использованием разработанного ИС с учетом варианта заданий.

Описание функциональных возможностей ИС.

1. ИС запрашивает пользователя о количестве систем для анализа. Число систем может быть 4 - 7. Каждая из систем располагается в своей матрице и ячейке. Выбор ячейки определяется параметрами, приведенными ниже.
2. Далее по каждой из систем ИС запрашивает следующие данные:

- вероятность киберинцидента (высокий (H), средний (M), низкий (L))
- тяжесть последствий киберинцидента (высокий (H), средний (M), низкий (L))

3. Все систем размещаются в индивидуальной матрице критичности. Положение для каждой из них определяется вероятностью и тяжестью. Всего 9 возможных положений в матрице.
4. Далее ИС предлагает определить информационные связи между системами. На картинке появляются линии со стрелками. Стрелка проводится от субъекта влияния к объекту влияния. Интерфейс программы должен позволять пользователю указать субъект и объект влияния. Таким образом формируется первоначальный граф критичности.
5. Далее программа предлагает определить степень этого влияния заполнив матрицу влияния между субъектом и объектом влияния. Направление стрелок указывает на то, между какими системами нужно определить влияния. Влияния между системами описывается в виде ЛП – Высокое, низкое, среднее.
6. ИС поддерживает обновление матриц критичности состояния ИБ путем проведения нечетких операций над ЛП

критичности и степени влияния с последующей ЛА к ближайшему нечеткому терму критичности.

7. После проведения нечетких операций и аппроксимации ИС должно выводить обновленный граф критичности.

В таблице 2.4 приведены варианты заданий.

Таблица 2.4 - Варианты заданий для аналитического отчета

№	Наименование объекта	Активы	Тип ФП для ЛП: Критичности и влияния
1.	Объект: Автоматизированная система управления дорожным движением транспорта	Активы: сервер базы данных, устройства управления дорожными знаками, канал связи, детектор транспорта, диспетчер, коммуникационный сервер, устройства управления светофорами	треугольная функция принадлежности
2.	Объект: Система управления уличным освещением	Активы: Канал связи, диспетчер, шкаф управления освещением, питающая подстанция, уличные фонари, сенсоры	трапециевидная функция принадлежности
3.	Объект: Система управления умным домом	Активы: датчики, сенсоры, коммутаторы, центральный контроллер, устройства управления, канал связи, пользователь, сервер контроля	треугольная функция принадлежности

Продолжение таблицы 2.4

№	Наименование объекта	Активы	Тип ФП для ЛП: Критичности и влияния
4.	Объект: Система удаленного мониторинга и управления объектами малой генерации	Активы: программно-технический комплекс, локально вычислительная сеть, удаленное рабочее место, канал связи, система автоматического управления энергоблоками	треугольная функция принадлежности
5.	Объект: автоматизированная система контроля и управления водоснабжением	Активы: SCADA-сервер, преобразователи гидростатического давления, преобразователи избыточного давления, модули ввода вывода, прибор контроля и управления задвижкой, блок сетевого фильтра, канал связи, оператор	трапециевидная функция принадлежности
6.	Объект: Система управления потоком тепловой энергии	Активы: Датчик температуры, расходомер, насос, коммутатор, канал связи, оператор	трапециевидная функция принадлежности

Продолжение таблицы 2.4

№	Наименование объекта	Активы	Тип ФП для ЛП: Критичности и влияния
7.	Объект: Система управления технологическими процессами	Активы: Сервер aswitch, канал связи, контроллеры, коммутаторы, датчики.	треугольная функция принадлежности
8.	Объект: Автоматизированная система управления транспортом	Активы: Коммутаторы, сервера, маршрутизатор, оператор, мультиплексоры	треугольная функция принадлежности
9.	Объект: Система дистанционного управления и контроля малых ГЭС	Активы: стойка автоматического управления гидроагрегатом, сервер сбора данных ССД-1, ADSL модем, Ethernet-коммутаторы, базовый спутник	трапециевидная функция принадлежности

Индивидуальная работа предусматривает подготовку каждым студентом аналитического отчета в соответствии с вариантом задания.

Требования к содержанию отчета.

Отчет должен содержать:

– титульный лист;

– цели и программу проведения исследований;

– описание этапов данного метода оценки ИБ смарт грид систем;

– скриншоты, подтверждающие работоспособность разработанного ИС;

– результаты оценки рисков ИБ для системы (по варианту);

– графики зависимости изменения критичности состояния ИБ объектов влияния от критичности субъектов влияния. Необходимо проанализировать все возможные цепочки развития киберинцидента;

– результаты анализа и выводы.

Контрольные вопросы

1. Назовите основные особенности матричных методов оценивания ИБ? В чем особенность их нечеткого расширения?
2. Что такое критичность состояния ИБ? Чем она обусловлена?
3. Назовите основные этапы метода?
4. Что понимается под лингвистическими переменными?
5. Что понимается под функцией принадлежности? Какого вида она бывает?
6. Что такое лингвистическая аппроксимация? Зачем она применяется?
7. Что такое нечеткое треугольное число? Какова его функция принадлежности?
8. Чем обусловлено использование методов нечеткого моделирования ИБ в смарт грид?
9. Какие основные преимущества и недостатки FMECA подхода?
10. Дайте основные рекомендации по снижению рисков ИБ для информационных систем? На чем должен быть основан выбор контрмер?

2.2 Практикум №2. Применение Fuzzy Logic Toolbox для анализа ИБ смарт грид систем

Форма занятия: практикум

Цель и задачи практикума является анализ ИБ смарт гри систем с использованием нечеткой логики.

Учебные задачи:

– изучение основных положений анализа ИБ и рисков с использованием нечеткой логики;

– изучение пакета Fuzzy Logic Toolbox.

Практические задачи:

– получение навыков применения пакета нечеткой логики Fuzzy Ligic Toolbox для исследования ИБ систем в смарт грид.

Исследовательские задачи:

- провести анализ рисков ИБ при исследовании аварий в индустриальных системах.

Подготовка к практикуму

При подготовке к практикуму необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [26-35].

Теоретический материал

С развитием концепции нейронных сетей и нечеткой логики "мягкое вычисление" лидирует в управлении сложными динамическими системами, по сравнению с классическими методами. Эта технология, включает в себя следующие направления: нечеткие множества (первого и второго рода); генетические алгоритмы; искусственный интеллект; моделирующие системы; вероятностное рассуждение; изучение алгоритмов интеллектуального управления; распознание образов;

самоорганизацию сложных систем; нечеткое управление; нечеткий информационный поиск и др.

Рассмотрим пример получения оценки критичности состояния с использованием прямого способа нечеткого вывода.

Рассмотрим решение задачи оценки критичности состояния системы на примере возможной атаки на транспортное средство (ТС).

Fuzzy Logic Toolbox – это пакет расширения MATLAB, содержащий инструменты для проектирования систем нечеткой логики.

Пакет позволят создавать экспертные системы на основе нечеткой логики, проводить кластеризацию нечеткими алгоритмами, а также проектировать нечеткие нейросети.

Пакет включает графический интерфейс для интерактивного пошагового проектирования нечетких систем, функции командной строки для разработки программ, а также специальные блоки для построения систем нечеткой логики в Simulink.

Все функции пакета написаны на открытом языке MATLAB, что позволяет контролировать исполнение алгоритмов, изменять исходный код, а также создавать свои собственные функции и процедуры.

Ключевые особенности:

– Графический интерфейс для интерактивного пошагового проектирования нечетких систем;

– Функции для создания экспертных систем на основе нечеткой логики;

– Поддержка логики И, ИЛИ и НЕ в настраиваемых правилах

– Стандартные типы экспертных систем нечеткой логики (Mamdani, Sugeno);

– Функции для нейроадаптивной и нечеткой кластеризации с обучением;

– Включение нечетких систем в Simulink-модели;

– Генерация С-кода и независимых приложений, реализующих системы нечеткой логики.

Ввод исходных данных

Рассмотрим иллюстративный пример определения критичности состояния ТС с использованием логико-лингвистического моделирования первого рода. Будем использовать несколько FIS - Multi Fuzzy Inference System (MFIS), для определения степени риска, используя факторы, связанные с каждым риском.

На данный момент злоумышленники и хакеры могут проникнуть в систему современного ТС как удаленно, так и непосредственно при помощи интерфейсов ТС, что может привести к рискам и ущербу. ER-модель ИБ атаки представлена на рис. 2.9.

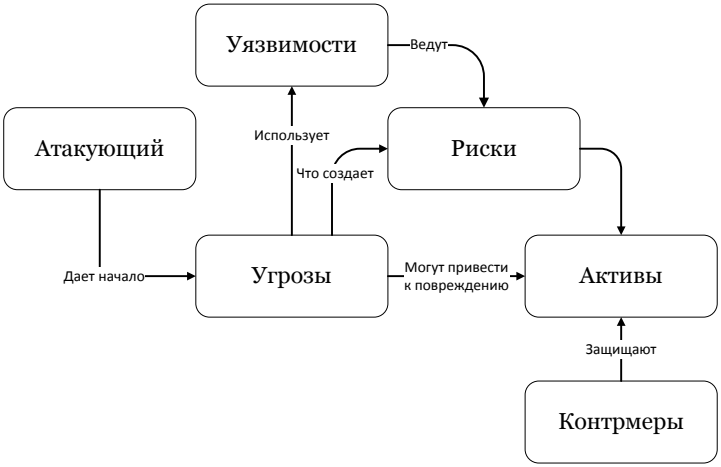


Рисунок 2.9 – ER -модель ИБ

Модель риска позволяет сформировать зависимости между параметрами нечеткого вывода, используемого для получения оценок риска.

Риски зависят от уязвимостей ТС (Vulnerability), вероятности использования этих уязвимостей (Action likelihood), и, наконец, вероятности успеха (Success likelihood).

Предлагается оценить риски ИБ в зависимости от общих возможностей, вероятности, безопасности (контрмер), возможности атаки на уязвимость, т.е.:

$$\text{Risk} = (\text{Possible and probable, Security, Impact}); \quad (2.5)$$

$$\text{OverallCapabilities} = (\text{Capabilities,Intent,Targeting}); \quad (2.6)$$

$$\text{OverallLikelihood} = (\text{Vulnerability, Action likelihood, Success likelihood}); \quad (2.7)$$

$$\text{Security} = (\text{Security data transmission, Security CAN-bus, Security each ECU}); \quad (2.8)$$

$$\text{Possible and probable} = (\text{Overall Capabilities, Overall Likelihood}). \quad (2.9)$$

где общие возможности - Overall Capabilities, общая вероятность атаки - Overall Likelihood, безопасность (контрмеры) - Security, возможности атаки на уязвимость с использованием возможностей - Possible and probable, воздействие на активы - Impact.

На основе модели риска, представленной уравнениями (см. выше) предлагается MFIS, которая состоит из пяти систем нечеткого вывода для оценки риска, как показано на рис. 2.10.

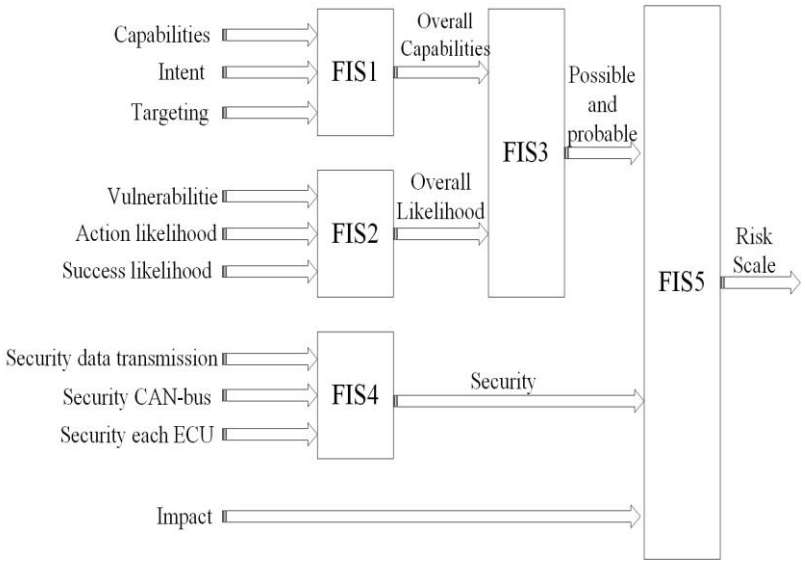


Рисунок 2.10 - Предлагаемая Multi Fuzzy Inference System (MFIS)

Первая нечеткая система логического вывода (FIS1) вычисляет OverallCapabilities источника угрозы, такого как экстремистская группа, террористическая группа, хакер или группа хакеров, на основе его (возможностей, намерений и ориентации).

Вторая система нечеткого логического вывода (FIS2) вычисляет OverallLikelihood угрозы в результате воздействия злоумышленника на основе факторов риска (уязвимости, воздействия на уязвимость, и вероятности успеха).

Третья система нечеткого логического вывода (FIS3) вычисляет PossibleAndProbable уязвимости на основании выхода FIS1 и FIS2.

Четвертая система нечеткого логического вывода (FIS4) вычисляет Security TC на основе (уровня защищенности передачи данных, уровня защищенности CAN-шин, уровня защищенности отдельных ECU).

Пятая система нечеткого логического вывода (FIS5) вычисляет RiskScale на основании выхода FIS3, FIS4 и уровня воздействия события угрозы, то есть величина ущерба, который можно ожидать (Impact).

Все нечеткие переменные выражаются грамматически в термах нечетких множеств, «Low», «Moderate», «High», как показано на рис. 2.11.

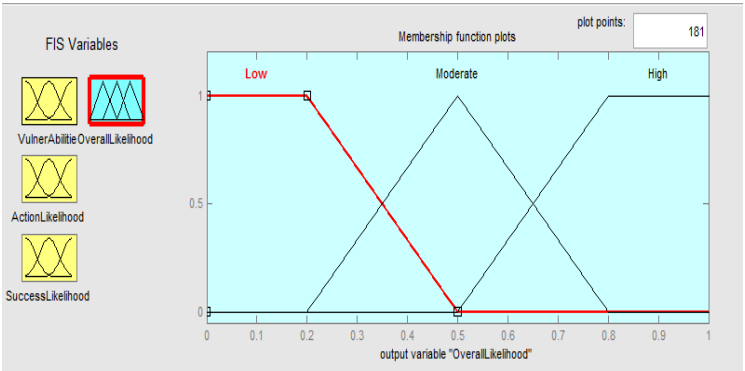


Рисунок 2.11 - Термы нечетких множеств

В этом исследовании ФП лингвистических термов характеризуются трапециевидной функцией принадлежности для «Low» и «High» и треугольной функцией принадлежности для «Moderate», поскольку именно такой набор функций позволяет дать оценку наиболее приближенную к количественным методам оценивания.

Таблицы 2.5 – 2.10 показывают значение термов ФП для каждого выхода MFIS.

Таблица 2.5 - Overall Capabilities

Терм	Значение
High (H)	Злоумышленник имеет высокий уровень знаний, со значительными ресурсами и возможностями для поддержки нескольких успешных скоординированных атак.

Moderate (M)	Злоумышленник имеет умеренные ресурсы, опыт и возможности для поддержки нескольких успешных атак.
Low (L)	Злоумышленник имеет ограниченные ресурсы, опыт и возможности для поддержки успешной атаки.

Таблица 2.6 - Overall Likelihood

Терм	Значение
High (H)	Злоумышленник с высокой вероятностью использует уязвимость для успешной атаки.
Moderate (M)	Злоумышленник с умеренной вероятностью использует уязвимость для успешной атаки.
Low (L)	Злоумышленник вряд ли использует уязвимость для успешной атаки.

Таблица 2.7 - Security

Терм	Значение
High (H)	Высокий уровень защищенности ECU, интерфейсов, CAN-шин, каналов передачи в ТС.
Moderate (M)	Умеренный уровень защищенности ECU, интерфейсов, CAN-шин, каналов передачи в ТС.
Low (L)	Низкий уровень защищенности ECU, интерфейсов, CAN-шин, каналов передачи в ТС.

Таблица 2.8 - Possible and probable

Терм	Значение
High (H)	Злоумышленник имеет высокую вероятность для успешной атаки на выявленную уязвимость.
Moderate (M)	Злоумышленник имеет среднюю вероятность для успешной атаки на выявленную уязвимость.
Low (L)	Злоумышленник имеет низкую вероятность для успешной атаки на выявленную уязвимость.

Таблица 2.9 – Impact

Терм	Значение
High (H)	Событие угрозы может привести к серьезным или катастрофическим неблагоприятным последствиям.
Moderate (M)	Событие угрозы может привести к умеренным негативным последствиям.
Low (L)	Событие угрозы может привести к незначительным отрицательным последствиям.

Таблица 2.10 - Risk Scale

Терм	Значение
High (H)	Данный риск означает, что событие угрозы может привести к серьезным или катастрофическим последствиям для ТС, пассажиров и других участников дорожного движения.
Moderate (M)	Данный риск означает, что событие угрозы может привести к умеренным негативным последствиям для ТС и пассажиров.
Low (L)	Данный риск означает, что событие угрозы может привести к незначительным отрицательным последствиям для ТС.

После начала работы пользователь видит стартовый экран Matlab (см. рис. 2.12).

Первое, что нужно сделать – это открыть Fuzzy Logic Toolbox. Открытие происходит при нажатии на кнопку Apps => Show more и выборе Fuzzy Logic Designer (Рисунок 2.12.):

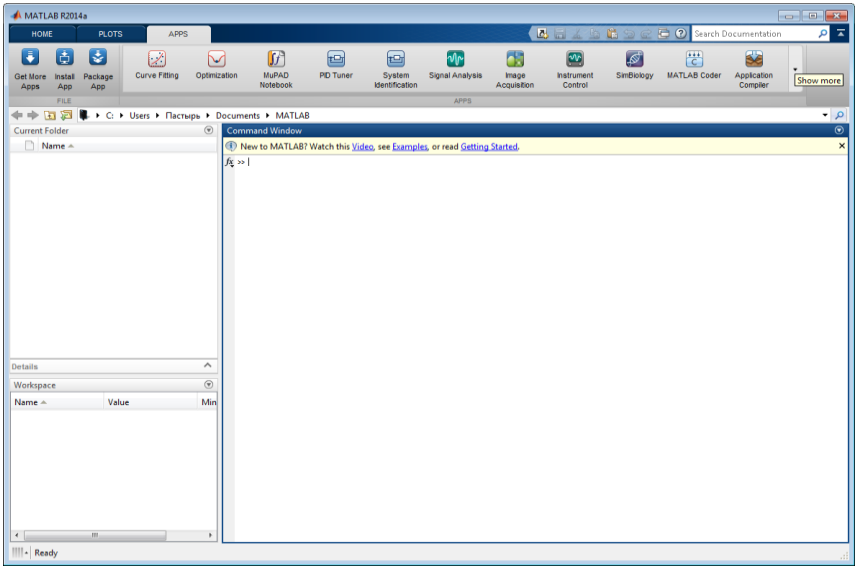


Рисунок 2.12 – Открытие Fuzzy Logic Toolbox (1)

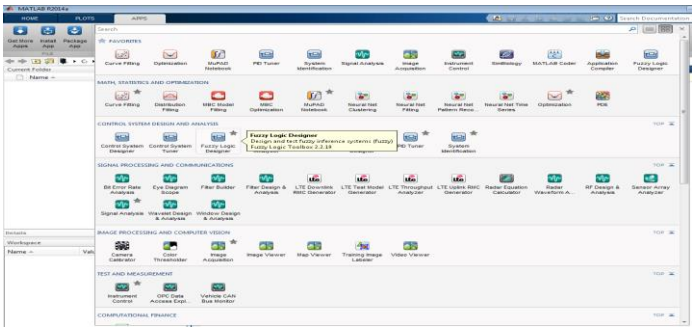


Рисунок 2.13 – Открытие Fuzzy Logic Toolbox (2)

Стартовая страница Fuzzy Logic Toolbox выглядит таким образом (Рисунок 2.14):

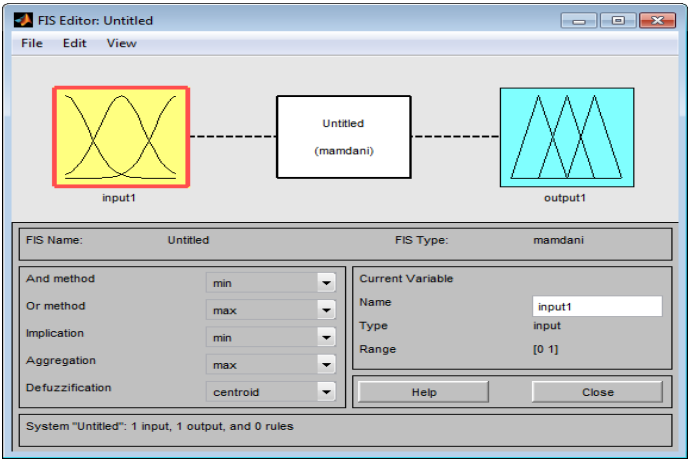


Рисунок 2.14 – Стартовая страница

где: **Input1** – входная переменная; **Output1** – выходная переменная; **Untilied** – это правила

Входные переменные

Для удобства работы необходимо переименовывать входные переменные. Для этого необходимо выделить переменную, которая нам нужна и в графе **name** указать имя. Остальные параметры оставляем по умолчанию.

Откроем входные переменные поочередно для каждой FIS и присвоим им значения, определенные в таблице 2.11, 2.12, 2.13, 2.14, 2.15.

Таблица 2.11 - Описание входных переменных Capabilities, Intent, Targeting в FIS – Overall Capabilities

№	ЛП	Унив. множ.	High (H)	Middle (M)	Low (L)
1.	Возможности, которые есть у злоумышленника	Capabilities	100 – 60 %	75 – 25 %	40 – 0 %
2.	Намерения, умысел злоумышленника	Intent	100 – 60 %	75 – 25 %	40 – 0 %
3.	Нацеливание (цель) злоумышленника	Targeting	100 – 60 %	75 – 25 %	40 – 0 %

Таблица 2.12 - Описание входных переменных Vulnerabilities, Action likelihood, Success likelihood в FIS2 – Overall Likelihood

№	ЛП	Унив. множ.	High (H)	Middle (M)	Low (L)
1.	Вероятность уязвимости ECU	Vulnerability	100 – 50 %	80 – 20 %	50 – 0 %
2.	Вероятность обнаружения и использования найденной уязвимости	Action likelihood	100 – 50 %	80 – 20 %	50 – 0 %
3.	Вероятность успеха воздействия на уязвимость	Success likelihood	100 – 60 %	75 – 25 %	40 – 0 %

Таблица 2.13 - Описание входных переменных Overall Capabilities, Overall Likelihood в FIS3 – Possible and probable

№	ЛП	Унив.множ.	High (H)	Middle (M)	Low (L)
1.	Общие возможности источника угрозы	Overall Capabil.	100 – 40 %	90 – 10 %	60 – 0 %
2.	Вероятность того, что данная угроза со стороны злоумышленника	Overall Likelihood	100 – 40 %	90 – 10 %	60 – 0 %

	способна использовать данную уязвимость (или набор уязвимостей)				

Таблица 2.14 - Описание входных переменных Security data transmission, Security CAN-bus, Security each ECU в FIS4 – Security

№	ЛП	Унив.множ.	High (H)	Middle (M)	Low (L)
1.	Уровень защищенности передачи данных	Security data transmission	100 – 40 %	90 – 10 %	60 – 0 %
2.	Уровень защищенности CAN шин	Security CAN-bus	100 – 40 %	90 – 10 %	60 – 0 %
3.	Уровень защищенности отдельных ECU	Security each ECU	100 – 40 %	90 – 10 %	60 – 0 %

Таблица 2.15 - Описание входных переменных Possible and probable, Security, Impact в FIS5 – Risk Scale

№	ЛП	Унив.множ.	High (H)	Middle (M)	Low (L)
1.	Возможность атаки на уязвимость	Possible and probable	100 – 40 %	90 – 10 %	60 – 0 %
2.	Уровень защищенности автомобиля	Security	100 – 50 %	80 – 20 %	50 – 0 %

№	ЛП	Унив.множ.	High (H)	Middle (M)	Low (L)
3.	Уровень воздействия события угрозы. Величина ущерба, который можно ожидать в результате последствий несанкционированного доступа, несанкционированной модификации или потери доступности контроля над автомобилем или отдельной информационной системы.	Impact	100 – 60 %	80 – 20 %	40 – 0 %

Выходные переменные

Производим изменение выходных переменных по такому же алгоритму, что и входных.

Таблица 2.16 - Описание выходных переменных Overall Capabilities, Overall Likelihood, Risk Scale

№	ЛП	Универсальное множество	High (H)	Middle (M)	Low (L)
1.	Общие возможности источника угрозы	Overall Capabilities	100 – 60 %	75 – 25 %	40 – 0 %

2.	Вероятность того, что данная угроза со стороны злоумышленника способна использовать данную уязвимость (или набор уязвимостей)	Overall Likelihood	100 – 50 %	80 – 20 %	50 – 0 %
3.	Возможность атаки на уязвимость	Possible and probable	100 – 40 %	90 – 10 %	60 – 0 %
4.	Уровень защищенности автомобиля	Security	100 – 40 %	90 – 10 %	60 – 0 %
5.	Шкала риска на основании выходов из FIS3, влияния Impact и Security.	Risk Scale	100 – 40 %	80 – 20 %	60 – 0 %

Описание правил

Логико-лингвистическое описание связей между входными и выходными переменными для FIS1 позволяет представить полученные знания в виде матрицы, представленной в таблице 2.17.

Таблица 2.17 - Правила для FIS1

Crt	Capabilities	Intent	Targeting
High (H)	H	H	H
H	H	H	M
H	H	M	H
H	M	H	H

H	H	H	L
H	H	L	H
H	M	M	H
H	M	H	M
H	H	M	M
H	H	L	L
Middle(M)	M	M	M
M	M	M	L
M	M	L	M
M	M	L	L
Low(L)	L	L	L
L	L	M	L
L	L	H	H
L	L	H	L
L	L	L	H
L	L	M	L
L	L	L	M
L	L	M	M

Таблица 2.18 - Правила для FIS2

Crt	Vulnerabilities	Action likelihood	Success likelihood
High (H)	H	H	H
H	M	M	H
H	H	M	H
H	M	H	H
H	H	M	M
H	M	H	M

Продолжение таблицы 2.18

H	M	M	M
H	H	H	M
Middle(M)	M	M	L
M	M	L	M
M	M	H	L

M	H	M	L
M	H	H	L
M	L	H	H
M	L	M	H
Low(L)	H	L	L
L	L	L	L
L	L	L	M
L	L	M	L
L	L	H	L
L	M	L	L
L	L	L	H

Таблица 2.19 - Правила для FIS3

Crt	Overall Capabilities	Overall Likelihood
High (H)	H	H
H	M	H
H	H	M
Middle(M)	M	M
M	L	H
M	H	L
Low(L)	L	L
L	M	L
L	L	M

Таблица 2.20 - Правила для FIS4

Crt	Security data transmission	Security CAN-bus	Security each ECU
High (H)	H	H	H
H	M	M	H
H	H	M	H

H	M	H	H
H	H	M	M
H	M	H	M
H	H	H	M
Middle(M)	L	M	H
M	M	M	M
M	M	L	M
M	M	H	L
M	H	M	L
M	H	H	L
M	L	H	H
Low(L)	H	L	L
L	L	L	L
L	L	L	M
L	L	M	L
L	L	H	L
L	M	L	L
L	L	L	H
L	M	M	L

Таблица 2.21 - Итоговая таблица правил

Crt	Possible and probable	Security	Impact
High (H)	H	L	H
H	H	M	H
H	H	M	M
H	M	L	H
Middle(M)	M	M	M
M	M	L	M
M	M	L	L
M	H	L	L
M	H	M	L
Low(L)	L	L	L
L	L	M	L
L	L	H	L

Crt	Possible and probable	Security	Impact
L	M	H	L
L	L	H	M
L	L	H	H
L	L	M	M

Далее, используя таблицы и операции $\wedge$ (И – min) и $\vee$ (ИЛИ – max) записывается система логических уравнений, которая связывает ФП оценки ИБ с переменными, которые влияют на нее.

Когда все правила будут заполнены, можно будет посмотреть результат анализа во вкладке **View (Rule/Surface)** (рисунок 2.15-2.18):

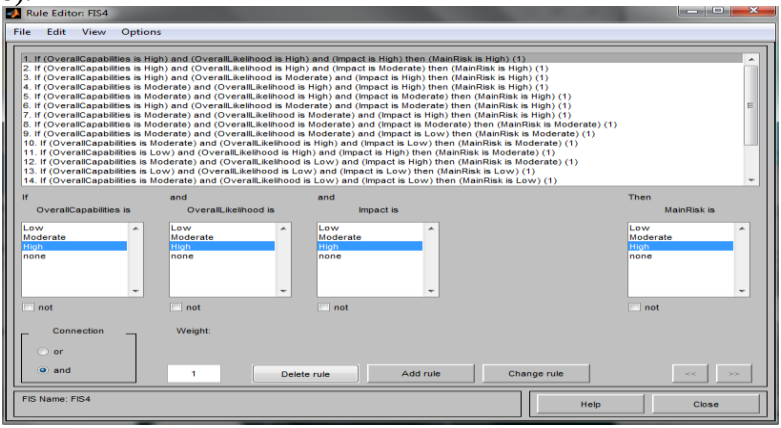


Рисунок 2.15 – Итоговая таблица правил

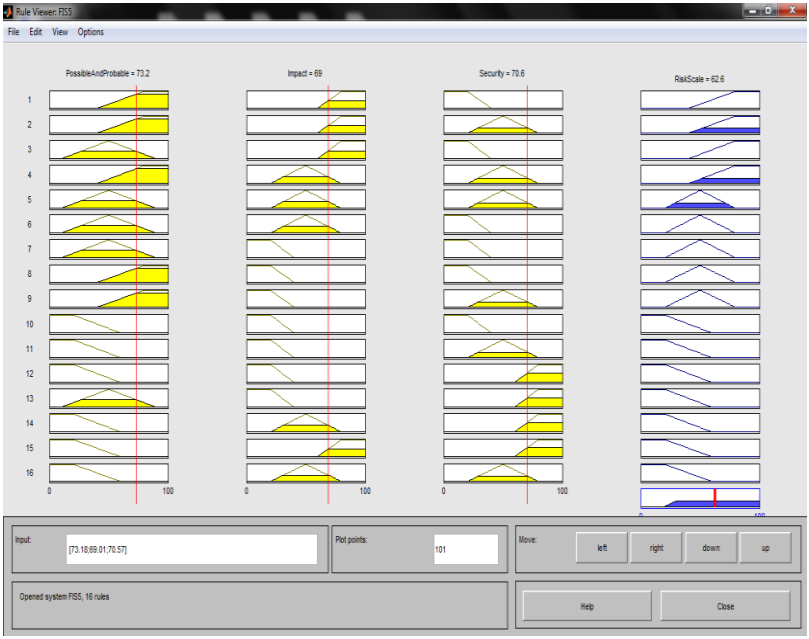


Рисунок 2.16 – Rule Viewer

Rule Viewer показывает графическое представление каждой из переменных через все правила, представление комбинаций правил. Например, как показано на рис. 11, для входов Possible and probable 73.2, Impact 69, и Security 70,6 - выходной уровень риска Risk Scale равен 62.6. Surface Viewer для FIS отображает 3-D граф, который показывает соотношение между входными переменными и выходной переменной. Surface Viewer показывает график возможных диапазонов входных переменных и возможный диапазон выхода.

На рис. 2.17 изображен 3D график для конечного результата RiskScale в зависимости от Impact и PossibleAndProbable. Видно, что значение переменных свыше 50% существенно и резко повышает риск кибербезопасности ТС.

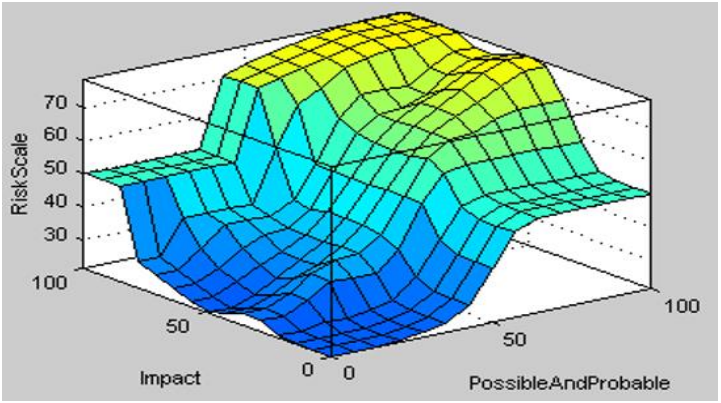


Рисунок 2.17 - Surface Viewer для
(Impact, PossibleAndProbable, and RiskScale)

На рис. 2.18 изображен 3D график для конечного результата RiskScale в зависимости от PossibleAndProbable и Security. Показано, что значение Security сравнивает влияние переменной PossibleAndProbable на общий риск кибербезопасности ТС.

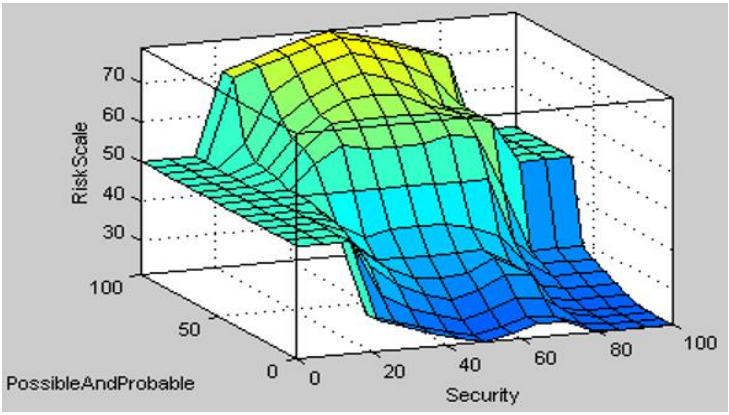


Рисунок 2.18 - Surface Viewer для
(PossibleAndProbable, Security and RiskScale)

На рис. 2.19 изображен 3D график для конечного результата RiskScale в зависимости от Security и Impact. Показано, что значение Impact хоть и растет, но существенно не влияет на общий риск ввиду высокго уровня Security.

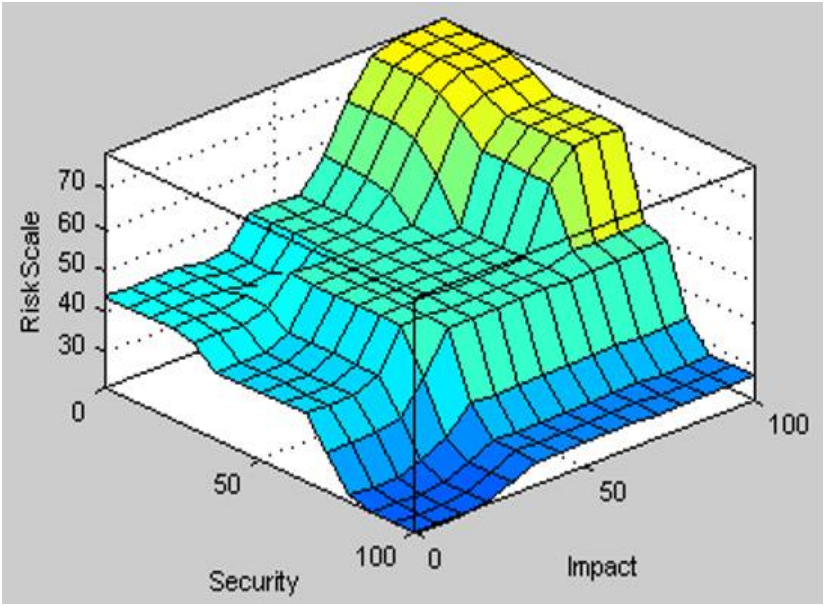


Рисунок 2.19 - Surface Viewer для
(Security, Impact and RiskScale)

Программа разработок

Практикум выполняется индивидуально. Результатом работы является подготовка аналитического отчета.

Аналитический отчет должен содержать:

1. Титульный лист.
2. Содержание
3. Цели и задачи проведения исследований;
4. Краткие теоретические сведения об аварии (см. таблицу 2.22).
5. Результаты анализа с использованием Fuzzy logic Toolbox;
6. Перечень возможных контрмер для снижения рисков ИБ.
7. Выводы.

Практикум завершается представлением презентации каждым студентом.

Таблица 2.22 - Варианты индивидуальных заданий для аналитического отчета

№	Вид ФП	Система нечеткого вывода	Наименование киберинцидента
1.	trimf - треугольная ФП	Сугено	Hacker Changes Chemical Plant Set Points via Modem
2.	trapmf - трапециевидная ФП	Мамдани	Proposed Hack of UK Water Systems
3.	gbellmf - обобщенная колокообразная ФП	Сугено	Utility SCADA System Attacked
4.	gaussmf - гауссовская функция принадлежности	Мамдани	Blockage of 12 Out Of 13 PLC Systems

Продолжение таблицы 2.22

№	Вид ФП	Система нечеткого вывода	Наименование киберинцидента
5.	gauss2m+ - двухсторонняя гауссовская ФП	Сугено	Change of Network Service Stopped OSI Layer-2 Communication
6.	sigmf - сигмоидная ФП	Мамдани	London August 2003 Power Blackout
7.	dsigmf - ФП в виде разности между двумя сигмоидными функциями	Сугено	SCADA Workstation Infected by W32/Korgo Worm
8.	gauss2mf - двухсторонняя гауссовская ФП	Мамдани	Worm attack on Drilling Control system
9.	dsigmf - ФП в виде разности между двумя сигмоидными функциями	Сугено	Whitehat Takeover of DCS Consoles
10.	gbellmf - обобщенная колокообразная ФП	Мамдани	German Steel Mill Cyber Attack
Примечание. Краткое описание киберинцидентов приведено по ссылке - http://www.risidata.com/Database			

Контрольные вопросы

1. Назовите основные особенности применения нечетких продукционных систем при решении задач анализа ИБ смарт грид?
2. В чем особенности построения многоуровневых систем нечеткого вывода оценивания ИБ смарт грид систем?
3. В чем отличия нечетких методов риск анализа ИБ от детерминированных?
4. В чем основные отличия методов нечеткой логики от вероятностных методов анализа ИБ?
5. Назовите основные функциональные возможности пакета Fuzzy Logic Toolbox?
6. Каким образом могут быть учтены контрмеры при оценивании ИБ с использованием нечеткой логики?
7. Назовите особенности системы выводы Сугено?
8. Назовите особенности системы выводы Мамдани? В чем ее отличия от Сугено?

3 ПРОЦЕССНО-ОРИЕНТИРОВАННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ ГРИД (ИУС)

3.1 Практикум №1. Изучение нормативной базы по обеспечению информационной безопасности ИУС (по требованиям US NRC)

Форма занятия: практикум

Цель и задачи практикума:

– изучение нормативной базы по обеспечению ИБ систем смарт грид (ИУС).

Учебные задачи:

– изучение содержания основных документов нормативной базы обеспечения ИБ смарт грид (ИУС).

Практические задачи:

– получение навыков логического анализа нормативной базы по обеспечению безопасности ИБ смарт грид и ИУС, важных для ее безопасности.

Исследовательские задачи:

Провести сравнительный анализ нормативной базы по обеспечению ИБ смарт грид (ИУС).

Подготовка к практикуму

При подготовке к работе необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [36-50].

Краткие теоретические сведения. *Анализ нормативной базы по обеспечению ИБ ИУС, важных для безопасности (на примере требований US NRC).*

ИУС АЭС являются примером индустриальных систем управления, к которым выдвигаются высокие требования к функциональной и информационной безопасности.

В США, Комиссия по ядерному регулированию (US NRC) в своей практике активно использует ряд документов, к наиболее важным из которых, с точки зрения ИБ ИУС, можно отнести следующие:

- 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”;
- NQA-1a-2009 Quality Assurance Requirements for Nuclear Facility Applications;
- Regulatory Guide (RG) 1.152-2011, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;
- IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”;
- IEEE Std 603-1991 “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”;
- DI&C-ISG-01, Revision 0, “Cyber Security Associated with Digital Instrumentation and Controls”;
- DI&C-ISG-06, Revision 1, “Licensing Process”;
- Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”;
- IEEE Std 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process”;
- NUREG/CR-7117, “Secure Network Design”;
- NIRMA TG-16;
- BTP 7-14, NUREG 6101.

Такие документы регламентируют множество аспектов, покрывая этапы, начиная с безопасной среды разработки и

эксплуатации и заканчивая свойствами безопасности критических систем, включая ИБ.

ИБ, в первую очередь, имеет непосредственное отношение к защитным мерам критических активов компании-разработчика, включая критические ИУС, от злоумышленных действий.

Рассмотрим некоторые положения приведенных выше документов.

10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

Стандарт по обеспечению качества в ядерной индустрии (NQA) является общим индустриальным стандартом, содержащим 18 критериев, соответствующих критериям 10 CFR 50 Appendix B. NQA описывает как должны быть построены все процессы, важные для безопасности, чтобы соответствовать требованиям 10 CFR 50 Appendix B.

Technical Guideline 16

Требования СМК в части ИБ усиливаются требованиями ряда документов типа Technical Guideline 16. Этот документ был разаботан Nuclear Information and Records Management Association (NIRMA) с целью обзора лучших практик управления записями.

Документ содержит требования к:

- разработке программы ИБ записей;
- управлению правами доступа;
- безопасности сети;
- управлению правами изменения содержания.

Стандарт IEEE Std 603-1991

Стандарт IEEE Std 603-1991 акцентирует внимание на

важности административных мер доступа к оборудованию ИУС, а также необходимости совместного использования средств ограничения физического и электронного доступа к критическим системам и данным с целью предотвращения несанкционированных изменений.

Отмечено, что безопасность программного обеспечения (ПО) компьютеризированных систем относится к возможности уцелеть вследствие несанкционированных, нежелательных, и небезопасных вмешательств на протяжении всего жизненного цикла таких систем.

Документы 10 CFR Part 50, Appendix B и 10 CFR 73.54, разработанные US NRC, представляют собой универсальные правила для лицензирования продукции и соответствующих предприятий на рынке США.

RG 1.152-2011 и RG 5.71-2010

Аспекты, относящиеся к кибер безопасности, покрываются документами RG 1.152-2011 и RG 5.71-2010. Первый из них описывает приемлемый с точки зрения US NRC метод, позволяющий реализовать процесс лицензирования использования компьютеров в системах безопасности атомных электростанций (АЭС). В частности, он содержит критерии установления безопасных сред разработки и эксплуатации цифровых ИУС посредством соответствующих физических, логических, программных и административных мер. Второй документ содержит непосредственное руководство по реализации активностей по защите компьютеров и коммуникационных систем и сетей. Он основывается на международных и федеральных стандартах и относится к этапам функционирования и обслуживания АЭС.

BTP 7-14

Документ BTP 7-14 представляет собой руководство по обзорам ПО для цифровых ИУС и содержит основные определения, касающиеся понятий безопасности и безопасности как функционального свойства. Вместе с тем он множество требований к документам планирования, каждый из которых содержит множество требований к ИБ.

Таким образом, существует множество требований к ИБ продукта. Их выполнение может быть достигнуто в рамках реализации одного из важных бизнес процессов компании – обеспечения ИБ. Дизайн процесса обеспечения ИБ должен проводится с учетом взаимосвязи с другими процессами в компании. Процесс обеспечения ИБ должен стать интегральной частью СМК компании.

Сравнительный анализ СМК с учетом требований к процессу обеспечения ИБ.

В общем случае, процесс обеспечения ИБ ИУС может быть реализован в рамках двух типов СМК: коммерческих и специальных (ядерных).

Коммерческие СМК. Традиционно, ИТ компании, не имеющие сертифицированный разрабатывающие продукт, к которому существуют требования ИБ не используют все возможности СМК в обеспечении ИБ конечного продукта. Как правило, рассматривается продуктовая составляющая ИБ (соответствие требованиям к ИБ продукта). В таких компаниях главный фокус делается на процесс тестирования безопасности для качества продукта. Представители групп верификации являются представителями контроля качества в компании.

Стандарты ISO серии 9001, описывающие модель СМК, разработаны для того, чтобы помочь организациям удовлетворять требования и ожидания клиентов и иных заинтересованных сторон.

В рамках ISO существует ряд требований, которые косвенно

можно отнести к требованиям ИБ. Так, требования по управлению документированной информацией включают необходимость обеспечения мер для:

- надлежащей защиты информации (например, от потери конфиденциальности, неправильного применения или потери целостности);
- управления документированной информацией (обеспечение доступа, хранение в надлежащем состоянии, контроль изменений, контроль версий);
- определения срока хранения и методов уничтожения. Документированная информация, сохраненная как свидетельство соответствия, должна быть защищена от непреднамеренных изменений.

Таким образом, в рамках ISO существует ряд требований к защите документированной информации от преднамеренных воздействий. Это единственное требование ИБ в рамках СМК ISO 9001.

Ядерные (Nuclear) СМК. Коммерческие СМК не выдвигают существенных требований к ИБ продукта. Более строгими в этом смысле являются специфические СМК, в которых главным фокусом является не удовлетворенность заказчика, а безопасность конечного продукта. В таких системах, важность уделяется бизнес процессам, важным с точки зрения выполнения продуктом функций безопасности.

Так, например, в США, компании, желающие продавать свой продукт на ядерном рынке, или стать поставщиком оборудования на АЭС должны иметь специфическую систему качества 10CFR50 Appendix B.

Ядерная СМК уделяет больше внимания аспектам ИБ, систем важных для безопасности. Так, например, указывается, что требования к ПО должны содержать специфические требования (защиту от уязвимостей, кибер безопасность, защиту от несанкционированного доступа, пр.). Аспект ИБ конечного продукта учитывается на всем ЖЦ ПО. Стандарт также выделяет

ряд отдельных требований к контролю доступа. Уделяется внимание безопасности сети и данных, требуется парольная защита.

Следует отметить, что поскольку ответственными за выполнение процедур и требований СМК являются менеджеры по качеству, то целесообразно усилить их вовлеченность в контроль процесса обеспечения ИБ.

Программа исследований и разработок

Работа выполняется индивидуально и коллективно. Индивидуальная работа предусматривает подготовку аналитического отчета по анализу стандарта. Студент выполняет роль бизнес-аналитика.

Аналитический отчет должен содержать:

- титульный лист;
- содержание отчета;
- перечень основных разделов стандарта;
- обобщенные требования по ИБ;
- примеры систем, для которых могут быть реализованы требования стандарта;
- пример требований по ИБ для выбранного примера системы.

Результаты выполнения индивидуального задания представляются в виде отчета.

Коллективное задание.

Каждая команда получает задачу, связанную с подготовкой учебного проекта по сравнительной оценке двух *нормативных документов* (в соответствии с вариантом).

Этапы создания учебного проекта:

1. Формирование команд (по списку учебной группы).
2. Выбор группы методов в соответствии с вариантом.
3. Постановка задач.
4. Внутрикомандная работа (подготовка презентации).
5. Презентация результатов.

Сравнительная оценка должна быть основана на системе обоснованных критериев, позволяющих сравнить документы нормативной базы. Критериями могут выступать: область действия стандарта, вид реализованного подхода (требования к продукту или процессу), “консерватизм”, перечень документов, предписанных стандартом, пр.

Таблица 3.1 - Варианты заданий для аналитического отчета

Вари-ант	Наименование стандарта по обеспечению безопасности
1.	10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
2.	NQA-1a-2009 Quality Assurance Requirements for Nuclear Facility Applications;
3.	Regulatory Guide (RG) 1.152-2011, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”
4.	IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”
5.	IEEE Std 603-1991 “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
6.	DI&C-ISG-01, Revision 0, “Cyber Security Associated with Digital Instrumentation and Controls”
7.	IEEE Std 7-4.3.2:2003
8.	DI&C-ISG-06, Revision 1, “Licensing Process”
9.	Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”
10.	IEEE Std 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process”
11.	NUREG/CR-7117
12.	NIRMA TG-16
13.	BTP 7-14
14.	NUREG 6101
Коллективная работа (сравнительный анализ вариантов)	
15.	вариант 1, 2

Вари-ант	Наименование стандарта по обеспечению безопасности
16.	вариант 3, 4
17.	вариант 5, 6
18.	вариант 5, 9
19.	вариант 1, 4
20.	вариант 4, 7

Контрольные вопросы

1. Назовите основные стандарты, регулирующие вопросы ИБ ИУС?
2. В чем их общее сходство (различия)?
3. Что такое процессное обеспечение ИБ?
4. Что понимается под “продуктным” обеспечением ИБ?
5. Выделите основные классификационные признаки стандартов по ИБ?
6. В чем отличие коммерческих и специальных (ядерных) систем менеджмента качеством с точки зрения требований по ИБ?
7. Что понимается под ИБ ПО? Чем оно обеспечивается? В чем особенность этапов ЖЦ с учетом требований по ИБ?
8. Какие проектные документы должны содержать требования по ИБ? Почему?
9. Может ли диверсность использоваться для обеспечения ИБ?

3.2 Тренинг. Процессный подход к обеспечению ИБ ИУС в смарт грид

Форма занятия: тренинг

Цели и задачи тренинга: изучение методики подготовки плана безопасной разработки и эксплуатации (ПБРЭ) программного обеспечения (ПО) ИУС, важных для безопасности, а также обзор нормативной базы, регулирующей разработку среды.

Учебные задачи:

– изучение процесса создания безопасной среды разработки и эксплуатации ПО ИУС, важного для безопасности;

– изучение нормативной базы, регламентирующей процессы безопасной среды разработки и эксплуатации при проектировании ПО;

– изучение требований, выдвигаемых к ИБ ПО ИУС, важных для безопасности.

Практические задачи:

– получение навыков формирования ПБРЭ;

– получение навыков оценки качества ПБРЭ с учетом параметров проекта по разработке ПО ИУС;

Исследовательские задачи*:*

– исследование возможностей по оценке и улучшению качества планов при разработке ПО, важного для безопасности.

Подготовка к тренингу

При подготовке необходимо:

1. Определение (выбор) темы задания с учетом варианта задания.

Задание включает выполнение двух подзадач: анализ и построение нормативного профиля требований ИБ к объекту разработки; разработка ПБРЭ для объекта с учетом варианта заданий и профиля требований.

Первое задание выполняется в ходе подготовки к тренингу. Его основная задача – формирование перечня требований к ИБ на основе анализа нормативной базы, регулирующей данные требования.

Второе задание – написание ПБРЭ для выбранного объекта разработки выполняется после проведения тренинга. Результат выполнения второй задачи – представленный ПБРЭ.

Студенты могут самостоятельно выбрать объект разработки и обосновать профиль требований по ИБ. В данном случае самостоятельный выбор должен быть согласован с тренером (преподавателем).

2. Разработка плана работ и распределение ответственности между участниками целевой группы.

План работ может быть представлен различными инструментами планирования расписания и управления сроками проекта:

– диаграммой Ганта (включает основные мероприятия, сроки и распределение ответственности между участниками целевой группы);

– методом критического пути (определение наиболее длительной последовательности задач от начала проекта до его окончания с учетом их взаимосвязи), пр.

Рабочая группа состоит из 4 человек. Распределение ответственности определяют участники группы.

Пример распределения ответственности: менеджер, осуществляющий планирование и координацию работ, а также представляющий идеологию работ в первой части общего доклада – постановку задачи, разработчики - системный аналитик, программист, менеджер по ИБ (отвечающий за выполнение мероприятий по контролю за ПБРЭ).

3. Поиск информации по теме работы.

При выполнении первого задания, связанного с анализом стандартов и другой регулятивной базы по ИБ, связанной с выбранным объектом разработки, поиск информации выполняется самостоятельно в Интернете.

4. Разработка плана отчета и презентации проекта.

План отчета (и презентации) включает подготовку следующих разделов:

– введение (актуальность проблемы обеспечения ИБ ИУС (индустриальных систем управления), краткий анализ инцидентов;

- формирование профиля требований по ИБ для выбранного объекта разработки;

– выводы (обоснования профиля требований);

– список литературы;

5. Написание отчета.

Отчет имеет объем 15-20 страниц формата А4 (шрифт 14, 1,5 инт., поля 2 см), включая титульный лист, содержание, основной текст, литература, приложения.

Обязательным приложением к отчету является план работ и распределение ответственности (диаграмма Ганта, метод критического пути, техника PERT), презентационные слайды и электронный вариант всех материалов.

6. Подготовка презентации.

Презентация разрабатывается и представляется в MS Power Point 2008, 2010 и соответствует плану обзора (10-15 слайдов) исходя из времени на презентацию – 15 мин.

Презентация должна включать следующие слайды:

– титульный слайд (с указанием ВУЗа, кафедры, дисциплины, темы доклада, автора, даты презентации);

– содержание (структура) доклада;

– актуальность вопросов ИБ выбранного объекта разработки;

– слайды с раскрытием профиля требований по ИБ;

– выводы по докладу;

– список использованных источников.

Каждый из слайдов должен содержать колонтитул с указанием темы и авторов доклада.

Подача информации может быть динамической.

7. Представление работы (первой части задания).

Защита работы осуществляется на тренинге, занимает 20 мин и включает собственно доклад с презентацией (15 мин) и обсуждение (5 мин).

8. Оценка работы.

Оценка выполненной работы учитывает качество текста отчета (форма и содержание), презентации (содержание и дизайн),

собственно доклад (структура, содержание и выводы), полноту, глубину и правильность ответов на вопросы.

Оценка за выполненную работу выставляется каждому студенту из группы авторов доклада индивидуально в соответствии с результатами и распределением ответственности.

Теоретический материал

Аспект кибер безопасности при разработке индустриальных систем, применяемых для управления производством или сложными технологическими процессами, становится актуальным. Это обусловлено возрастающим количеством кибер инцидентов, связанных с атаками на системы типы SCADA.

Анализ тенденций указывает на устойчивый рост числа атак на индустриальные системы, начиная с 2010 г. (после Stuxnet). Так, в феврале 2011 г. была проведена массивная атака «Night Dragon" на пять компаний по переработке нефти. В 2012 г. в ряде крупных компаний, работающий в банковской сфере Сирии, Ливана, Судана, было обнаружено вредоносное ПО ("Flame"), предназначено для выполнения шпионских действий, записи переговоров, пр. Таким образом, очевидна тенденция роста числа атак на индустриальные системы, которая в будущем будет сохраняться.

Разработчики индустриальных систем стремятся повысить их защищенность от внешних атак, снизить риски для кибер безопасности и потенциальные уязвимости. Имплементируя требования ИБ к системам, разработчики стремятся разработать безопасный продукт. Множество требований к ИБ можно разделить на: требования регулятора, нормативной базы, заказчика, пр. Очень часто, общая группа требований является несогласованной, не гармонизированной. Для компаний-разработчиков приложений одной из первоначальных задач является анализ требований, их систематизация и определение их приоритетов.

С учетом результатов этого анализа, компания-разработчик стремится разработать практические подходы, направленные на

выполнение всего множества требований.

Следует отметить, что анализ требований и разработка подходов не являются единичными (отдельными) задачами. Очень часто приходится иметь дело со множеством согласованных задач, выходы и входы которых взаимосвязаны между собой. Таким образом, можно говорить о необходимости дизайна (разработки) процесса обеспечения ИБ продукта в компании. Такой процесс является, по сути, одним из важных бизнес процессов компании, направленных на достижение удовлетворенности заказчика свойствами конечного продукта, на его кибер безопасность. Дизайн эффективного процесса обеспечения ИБ продукта может быть основан на использовании подходов к инжинирингу бизнес процессов.

При разработке процессов ИБ в компании необходимо учитывать ресурсы компании, уровень подготовки персонала, требования к продукту, зрелость используемых технологий, пр. Важной основой для дизайна процесса является СМК, которая является важнейшей составляющей системы управления бизнесом. Она содержит описание всех бизнес процессов компании, направленных на получение качественной продукции.

Поскольку обеспечение ИБ также является важным бизнес процессом компании, то его дизайн необходимо проводить с учетом других процессов компании в рамках системы менеджмента качеством.

Дизайн процесса обеспечения ИБ приложений на основе СМК.

В рамках дизайна процесса обеспечения ИБ на основе СМК целесообразно создать:

- процедуры и рабочие инструкции по обеспечению безопасности;
- политику компании, направленную на разработку безопасных приложений;
- программу тренингов с персоналом.

Процедура описывает процесс создания безопасных приложений. Цель процедуры предоставить руководство для проектирования безопасных приложений, с целью минимизации всех возможных уязвимостей, которые могут привести к невыполнению функций безопасности. Этот документ качества описывает методологию, направленную на выполнение требований по надежности, функциональной безопасности, качества ПО, на создание безопасной среды разработки и эксплуатации. Документ описывает мероприятия, направленные на создание безопасной среды разработки приложения, ее защиты от недокументированных, нежелательных модификаций, защитных мер против любых действий, направленных на снижение рисков для надёжности, безопасности при эксплуатации.

Важной частью процесса обеспечения ИБ является создание среды для безопасной разработки и применения. В рамках проекта разрабатываются план и отчет по обеспечению ПБРЭ.

Подход к реализации безопасных сред разработки и эксплуатации для процесса обеспечения ИБ.

Безопасная среда разработки определена как условие наличия соответствующих физических, логических и программных мер во время этапов разработки системы (рис. 3.1) для обеспечения невнесения нежелательной, излишней и недокументированной функциональности (например, избыточного кода) в цифровые системы, критические с точки зрения безопасности.

Безопасная среда функционирования определена как условие наличия соответствующих физических, логических и административных мер на предприятии для обеспечения надежного функционирования ИУС посредством отсутствия их деградации вследствие некорректного поведения подключенных систем, а также событий, порожденных непреднамеренным доступом к таким ИУС.

Для обоих сред, в общем случае, основными типами

компонент являются следующие:

- аппаратное обеспечение (включая технические средства функционирования и обеспечения безопасности инфраструктур сред разработки и эксплуатации, оборудование разработки и эксплуатации);
- программное обеспечение (включая то, которое относится к процессам разработки и эксплуатации, а также непосредственно к рассматриваемым инфраструктурам);
- сеть передачи данных (относящаяся как к среде разработки, так и эксплуатации);
- персонал;
- продукт (ИУС, которая разрабатывается и затем эксплуатируется).

Кроме вышеперечисленных типов компонент, немаловажным аспектом, подлежащим отдельному детальному анализу, является их конфигурация, которая включает множество факторов, охватывающих физические, логические и поведенческие взаимосвязи. Конфигурация в значительной степени зависит от качества и полноты внедрения СМК в средах разработки и эксплуатации, квалификации персонала, качества используемых программных и аппаратных компонент.

Реализация ПБРЭ, в контексте документа RG 1.152-2011, относится к следующим аспектам:

- предпринятым мерам и средствам по реализации безопасной среды для разработки ИУС, критических с точки зрения безопасности, предотвращающим недокументированные, избыточные и нежелательные изменения;
- защитным мерам, предотвращающим предсказуемый набор нежелательных действий, которые могут повлиять на целостность, надежность или функциональность ИУС во время ее функционирования.

Фазы каскадной модели жизненного цикла позволяют сформировать структуру специальных руководств по защите

цифровых систем, критических с точки зрения безопасности, а также по реализации ПБРЭ посредством идентификации и смягчения потенциальных недостатков либо уязвимостей в каждой из фаз, которые могут привести к деградации или снижению надежности таких систем.

Аудиты безопасности являются неотъемлемой частью процесса обеспечения безопасности во время разработки, реализации и поддержания ПБРЭ. Такие аудиты включают:

- аудит среды разработки: после учреждения инфраструктуры, в которой будет производиться разработка, и до начала проекта разработки ИУС;

- периодические аудиты: до начала каждой из фаз разработки.

Аудит среды разработки предназначен для оценки «базового» уровня безопасности среды разработки; преимущественно, соответствующие меры реализуются техническими средствами и относятся к сетям такой инфраструктуры, задействованным в процессе разработки, физическим средствам защиты и т.д.

В свою очередь, периодические аудиты предназначены для оценки дополнительных специфических мер, требуемых при реализации каждой из фаз разработки в жизненном цикле. Каждый из таких аудитов включает следующие этапы:

- проверка реализации дополнительных мер для фазы разработки (т.е. что реализовано и как);

- проверка соблюдения руководств и инструкций организации, относящихся к безопасной среде разработки, персоналом (т.е. практическая оценка того, следуют ли сотрудники соответствующим требованиям СМК).

Входом для каждого из аудитов является соответствующий план (и, возможно, документы, относящиеся к определенным аспектам организации среды разработки либо реализации процессов), а выходом – отчет по аудиту ПБРЭ, в котором задокументированы полученные результаты.

Обеспечение ИБ является важным бизнес-процессом

компании. Его дизайн (разработку) необходимо проводить с учетом специфики компании, ее ресурсов и используемых технологий. Выходом этого процесса является продукт, удовлетворяющий заказчика с точки зрения качества. Процесс обеспечения ИБ должен быть реализован в рамках СМК компании. При дизайне процесса обеспечения ИБ необходимо создать безопасную среду разработки приложений. Основой для разработки безопасного приложения может стать создание безопасной среды разработки, основой которой может быть ядерная СМК и ее принципы.

Специалисты по ИБ компании должны работать вместе со специалистами по качеству, уделяя внимание проблемам безопасности приложений, управлению доступом, управлению записями и документами. Важно иметь специалистов по качеству, понимающих важность рисков ИБ. СМК – ориентирована на ИБ, группа ИБ – ориентирована на качество.

Важным аспектом является внесение процесса создания и контроля безопасной среды разработки непосредственно в СМК. Таким образом, контроль разработки безопасной системы является совместной ответственностью менеджеров по качеству и специалистов по ИБ в компании.

С учетом вышесказанного, ПБРЭ определяет основные группы активностей, а именно:

1. Активности, связанные с обеспечением безопасности ПО ИУС в среде эксплуатации (относятся к разрабатываемой системе):

- анализ уязвимостей среды эксплуатации ИУС;
- формирования перечня проектных свойств ИУС, относящихся к безопасности;
- разработка требований к безопасности и конфигурации системы (как часть общих требований к системе);
- преобразование спецификации требований к системе в специфические компоненты конфигурации проекта системы (и их документирование в описании проекта);

- преобразование проекта системы в код, структуры данных и связанные с ними исполнимые машинные представления;

- тестирование интегрированных в систему проектных требований, относящихся к безопасности.

2. **Активности, связанные с обеспечением безопасности в среде разработки** (относятся к инфраструктуре, в которой реализуется процесс разработки):

- анализ уязвимостей среды разработки. Реализация мер безопасности в среде разработки и компьютерной сети;

- меры по защите процессов разработки требований и документации от включения излишних или инородных требований

- меры по обеспечению предотвращения включения в проект системы излишних особенностей или функций;

- меры по минимизации и смягчению любых случайных или несоответствующих изменений в проекте системы (корректное, точное и полное преобразование проекта в код);

- меры по валидации всех проектных свойств системы, относящихся к безопасности.

Тренинг состоит из нескольких частей.

Студенты принимают участие в тренинге по формированию ПБРЭ. Целью этой части тренинга является формирование необходимых знаний и практических навыков по подготовке ПБРЭ для выбранного объекта разработки.

Третья часть включает в себя разработку и представление планов ПБРЭ в соответствии с шаблоном, изученным в ходе второй части тренинга.

Отчетность по тренингу включает в себя разработку проекта ПБРЭ с учетом варианта заданий.

Для представления результатов исследований, необходимо подготовить и провести презентацию.

Варианты заданий (тем) приведены в таблице 3.2.

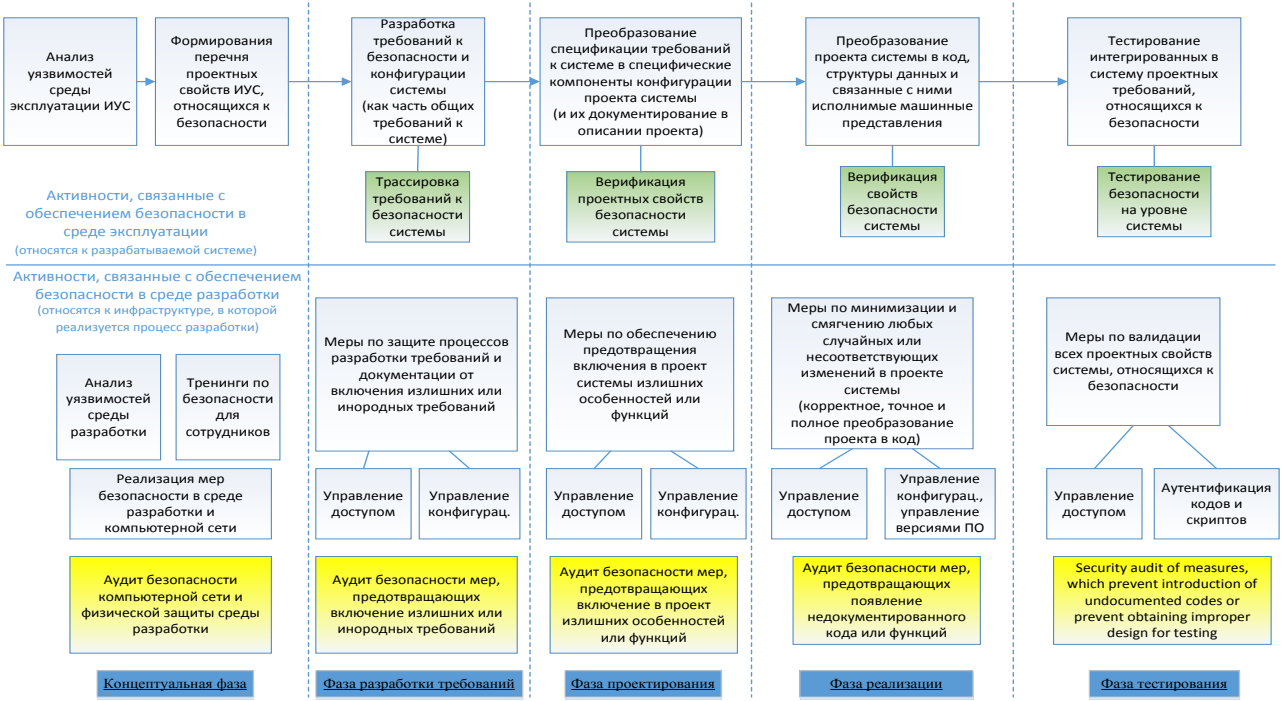


Рисунок 3.1 - Детализация активностей по обеспечению безопасных сред разработки и эксплуатации

Таблица 3.2 – Варианты заданий

Вариант	Наименование объекта	Активы/Описание
1.	Цифровая подстанция	http://www.gegridsolutions.com/alstomenergy/grid/Global/OneAlstomPlus/Grid/PDF/
2.	ПЛК	http://www.intechnics.ru/plc.html
3.	Объект: Автоматизированная система управления дорожным движением транспорта	Активы: сервер базы данных, устройства управления дорожными знаками, канал связи, детектор транспорта, диспетчер, коммуникационный сервер, устройства управления светофорами
4.	Температурный контроллер	http://www.intechnics.ru/termocontrollers.html
5.	Программируемый контроллер	http://www.intechnics.ru/products_delta_dvpes2.htm
6.	Объект: Система управления уличным освещением	Активы: Канал связи, диспетчер, шкаф управления освещением, питающая подстанция, уличные фонари, сенсоры. http://www.sicon.ru/prod/asuno/
7.	“Умный” счетчик	http://www.sanxingelectric.com/prodeta.php
8.	Объект: Система удаленного мониторинга и управления объектами малой генерации	Активы: программно-технический комплекс, локально вычислительная сеть, удаленное рабочее место, канал связи, система автоматического управления энергоблоками.

Продолжение таблицы 2.2

Вариант	Наименование объекта	Активы/Описание
9.	Объект: автоматизированная система контроля и управления водоснабжением	Активы: SCADA-сервер, преобразователи гидростатического давления, преобразователи избыточного давления, модули ввода вывода, прибор контроля и управления задвижкой, блок сетевого фильтра, канал связи, оператор.
10.	Объект: Система управления потоком тепловой энергии	Активы: Датчик температуры, расходомер, насос, коммутатор, канал связи, оператор.
11.	Объект: Система управления технологическими процессами	Активы: Сервер aswitch, канал связи, контроллеры, коммутаторы, датчики.
12.	Объект:Автоматизированная система управления транспортом	Активы: Коммутаторы, сервера, маршрутизатор, оператор, мультиплексоры

Требования к финальному отчету.

Аналитический обзор имеет объем 15-20 страниц формата А4 (шрифт 14, 1,5 интервал, поля 2 см), включая титульный лист, содержание, основной текст, литература, приложения.

Обязательным приложением к обзору является план работ и распределение ответственности (диаграмма Ганта, метод критического пути, техника PERT), слайды презентации и электронный вариант всех материалов.

Контрольные вопросы

1. На каких этапах должны быть реализованы требования по ИБ к готовому продукту?
2. В чем состоит анализ среды разработки, выполняемый на этапе разработки концепции системы?
3. Какой этап предшествует формированию перечня проектных свойств ИУС, относящихся к безопасности?
4. Как гарантируется выполнение требований к ИБ на этапе преобразования проекта системы в код, структуры данных и связанные с ними исполнимые машинные представления?
5. Как может быть реализован этап тестирования интегрированных в систему проектных требований, относящихся к безопасности?
6. Что понимается под аудитом безопасности компьютерной сети и физической защиты среды разработки?
7. Назовите основные меры по защите процессов разработки требований и документации от включения излишних или инородных требований?
8. Перечислите основные меры по валидации всех проектных свойств системы, относящихся к безопасности
9. В чем состоит управление доступом к информационным ре сурам ИУС?
10. Что понимается под аутентификацией кодов и скриптов?

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

4.1 Пояснения к учебной программе

Самостоятельную работу над дисциплиной «**Основы анализа и обеспечения информационной безопасности смарт грид**» («**Fundamentals of smart grid information security analysis and assurance**») следует начинать с изучения учебной программы, которая приведена в данном Приложении. Эта программа включает следующие элементы.

Объект изучения – смарт грид, как одно из самых перспективных направлений в области современной энергоэффективности, связанное с повышением надежности, энергосбережения, информационной безопасности и экономии расходов.

Предмет изучения – общие принципы, методы, ИС анализа и обеспечения ИБ систем в смарт грид (ИУС).

Требования к исходным знаниям и навыкам, которые необходимо иметь перед началом изучения:

– принципы и методы системного анализа;

– теория нечетких множеств;

– основные положения теории риск анализа;

– базовые знания в области современных компьютерных систем и информационных технологий.

Целью изучения дисциплины является приобретение студентами теоретических знаний и навыков оценивания рисков и ИБ при проектировании систем смарт грид (ИУС), использование инструментальных средств анализа и оценивания ИБ.

В результате ее изучения обучаемые должны научиться:

– проводить анализ получаемой информации и синтезировать на основе этого качественно новую информацию;

– правильно формулировать, четко и ясно задавать вопросы и соответственно уметь грамотно отвечать на поставленные вопросы;

– мыслить креативно и критически;

– предпринимать исследовательские действия и оценивать получаемые результаты с использованием качественных и количественных показателей;

– формулировать возможные практические решения проблемы, эффективно использовать время и доступные ресурсы для достижения целей дисциплины;

– демонстрировать гибкость, инициативу, умение выражать свое мнение;

– реализовывать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;

– применять перспективные методы оценивания рисков ИБ систем смарт грид (ИУС);

– применять ИС анализа и оценивания ИБ в смарт грид системах (ИУС).

Вследствие изучения дисциплины обучаемые обязаны:

1) теоретический компонент:

– получить базовые представления о сфере проблем, связанных с информационными технологиями, используемыми при анализе и оценивании ИБ смарт грид;

– иметь представление о методах, принципах и подходах, используемых при анализе ИБ систем в смарт грид;

– иметь представление о ИС, используемых при при оценивании ИБ;

– получить базовые представления о нормативной базе, используемой при проектировании систем с повышенными требованиями по ИБ.

2) познавательный компонент:

– знать основные принципы риск анализа в сложных динамических системах, подходы к оптимизации параметров энергосистем;

– знать базовые положения стандартов по обеспечению ИБ смарт грид (ИУС);

– знать базовые положения анализа ИБ смарт грид (ИУС);

– знать методы нечеткого анализа ИБ сложных систем;

3) практический компонент:

– уметь использовать методы матричного анализа ИБ ;

– уметь использовать методы нечеткого анализа безопасности смарт грид (ИУС);

– уметь анализировать и формировать профиль требований по ИБ смарт грид (ИУС).

Структура и содержание модулей. Дисциплина включает три модуля:

МОДУЛЬ 1. МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ ГРИД

Лекции

ТЕМА 1. Введение в теорию информационной безопасности смарт грид систем и их ИУС. Новые проблемы и вызовы

ТЕМА 2. Анализ методов риск менеджмента ИБ смарт грид.

ТЕМА 3. Применение информационных технологий для поддержки и принятия решений при проектировании смарт грид и их ИУС с учетом рисков ИБ.

Семинар (4 ч). Обзор инструментальных средств риск анализа ИБ смарт грид (ИУС)

Практикум (4 ч.) Ознакомление с инструментальными средствами анализа рисков ИБ смарт грид. Изучение Secur*IT*ree

МОДУЛЬ 2. НЕЧЕТКИЕ МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 1. Обзор подходов к нечеткому оцениванию ИБ смарт грид (ИУС).

ТЕМА 2. Нечеткие расширения качественных методов оценивания ИБ ИУС.

Тема 3. Обзор инструментальных средств нечеткой оценки рисков и ИБ.

Практикум 1. Применение матричных методов для нечеткой оценки рисков кибер инцидентов систем в смарт грид (4 ч.)

Практикум 2. Анализ ИБ смарт грид с использованием Fuzzy Logic Toolbox (4 ч.)

МОДУЛЬ 3. ПРОЦЕССНО-ОРИЕНТИРОВАННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ ГРИД (ИУС)

Лекции

ТЕМА 1. Анализ нормативной базы по ИБ ИУС, важных для безопасности и надежности смарт грид.

ТЕМА 2. Методы и средства обеспечения ИБ ИУС в смарт грид.

ТЕМА 3. Процессное обеспечение ИБ ИУС в смарт грид.

Практикум №1. Изучение нормативной базы по обеспечению информационной безопасности ИУС (по требованиям US NRC) (4 ч.)

Тренинг. Процессный подход по обеспечению ИБ ИУС в смарт грид (4 ч.)

Методы оценки
Экзамен (100 %).
По окончании курса проводится 90-минутный экзамен.

Отчетность по дисциплине включает отчеты по каждому виду практического занятия, а также экзамен, который включает типовые вопросы и задачи.

4.2 Подготовка к занятиям и экзамену

При подготовке к практикам (семинарам) следует обратить внимание на уяснение целей и задач (учебных или теоретических, практических и исследовательских) и знаний, которые нужны для их выполнения. Особое внимание следует уделить формулировке выводов по результатам исследований при оформлении отчета. При самостоятельной подготовке к занятиям важно правильно спланировать как свою индивидуальную, так и коллективную работу, организовать отбор и анализ необходимой литературы, подготовку к ответам на вопросы, приведенные в каждом разделе.

Следует обратить внимание на вопросы, вынесенные на самостоятельное изучение, которые приводятся в программе и уточняются преподавателем.

4.3 Вопросы для самостоятельной работы

1. Назовите ключевые информационные и коммуникационные технологии смарт грид, характеризующихся наибольшей уязвимостью? Почему? Основные группы уязвимостей?
2. Назовите основные регулятивные документы (стандарты, положения, пр.) регламентирующие вопросы обеспечения информационной безопасности систем смарт грид?
3. Назовите основные высокоуровневые требования к информационной безопасности смарт грид? Сформулируйте основные требования по ИБ к ИУС критического применения? В чем отличия?

4. Сформулируйте основные особенности физической безопасности систем в смарт грид?

5. Назовите основные методы тестирования безопасности смарт грид систем? В чем их основные особенности?

6. Назовите основные группы коммуникационные протоколы, используемые в смарт. Каковы признаки ИБ смарт грид?

7. В чем основное отличие методов анализа ИБ смарт грид и функциональной безопасности для ИЭИ?

8. Каковы возможные подходы к проведению совместного анализа ИБ и ФБ в смарт грид?

ЛИТЕРАТУРА

1. V. Kharchenko, V. Sklyar, E. Brezhniev, 2013, Safety of information and control systems. Models, techniques and technologies – Palmarium Academic Publishing, pp. 528.
2. R. Bloomfield, K. Netkachova, R. Stroud, 2013, “Security-Informed Safety: If It’s Not Secure, It’s Not Safe”, Software Engineering for Resilient Systems Lecture Notes in Computer Science, Volume 8166, Springer Berlin Heidelberg, pp. 17-32.
3. Yastrebenetsky, M., Kharchenko, V., 2014, “Nuclear power plant instrumentation and control systems for safety and security”, IGI Global, pp. 470.
4. M. Yastrebenetsky, V. Kharchenko (Edits), “*Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*”, A volume in the Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series, Hershey, Pennsylvania, United States of America, IGI Global, 2014, 470 p.
5. Huffmire, C. Irvine, T.D. Nguyen, “*Handbook of FPGA Design Security*”, Springer, 2010, 177 p.
6. V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora, “Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context”, Proceedings of the International Conference on Information and Digital Technologies (IDT 2015), Žilina, Slovakia, July 7-9, 2015, pp. 117-123.
7. Momoh, J. A, "Fundamentals of analysis and computation for the Smart Grid," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-5, 25-29 July 2010.
8. Arnold, G. W, "Challenges and Opportunities in Smart Grid: A Position Article," Proceedings of the IEEE, vol.99, no.6, pp.922-927, June 2011.
9. [Электронный ресурс]: режим доступа ttps://www.cyberriskanalytics.com/
10. [Электронный ресурс]: режим доступа: https://www.riskwatch.com/
11. [Электронный ресурс]: режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-

management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
12. [Электронный ресурс]: режим доступа: http://www.security-risk-analysis.com/introcob.htm
13. [Электронный ресурс]: режим доступа: http://www.amenaza.com/index.php
14. Надеждин, Ю. В. Безопасность АСУ ТП критически важных объектов [Электронный ресурс] / Ю.В. Надеждин – Режим доступа: http://www.uipdp.com/articles/2014-04/06.html
15. ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary (IDT).
16. Воронцов, А.Л. Автоматизированные системы управления технологическими процессами. Вопросы безопасности [Электронный ресурс]/А.Л Воронцов –Режим доступа: http://www.jetinfo.ru/stati/informatsionnaya-bezopasnost-promyshlennykh-obektov.
17. NIST Cybersecurity Framework [Электронный ресурс] – режим доступа: http://www.nist.gov/cyberframework/upload/cybersecurity-framework.
18. NISTIR 7628 Guidelines for Smart Grid Cyber Security[Электронный ресурс] – режим доступа: www.nist.gov/smartgrid/upload/nistir-7628.
19. Юдин, А.А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности SMART GRID систем [Электронный ресурс] / А.А. Юдин, Г. В. Пирогов – Режим доступа: pnzzi.kpi.ua/25/25_p88.pdf.
20. McQueen, M. Quantitative Cyber Risk Reduction Estimation Methodology For A Small SCADA Control System [Электронный ресурс] / M. McQueen, Boyer W., Flynn M., Beitel G. – Режим доступа: http://www.inl.gov/technicalpublications/Documents/3303778.
21. NIST SP800-30 Risk Management Guide for Information Technology Systems Text]. – National Institute of Standards and Technology 2002 – 95 p.

22. Byres, E. J., Franz, M. and Miller, D., “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems”, International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, December 4, 2004.
23. Scambray, J. and McClure, S., “Hacking Exposed Windows 2000: Network Security Secrets and Solutions,” McGraw_Hill, 2001.
24. B. Utne, P. Hokstad, G. Kjolle, J. Vatn, I.A. Tendel, D. Bertelsen, H. Fridheim, J. Rustrum, Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS approach.
25. U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.
26. The MathWorks. [online]. Fuzzy Logic Toolbox. Available: http://www.mathworks.com/products/fuzzylogic/ [Dec 16, 2005].
27. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg, 2015.
28. V. Novak, Mathematical fuzzy logic in modeling of natural language semantics, in: P. Wang, D. Ruan, E. Kerre (Eds.), Fuzzy Logic – A Spectrum of Theoretical & Practical Issues, Elsevier, Berlin, 2015.
29. Sirigiri, P., & Gangadhar, P.V., & Kajal, K.G. Evaluation of teacher’s performance using Fuzzy Logic Techniques. International Journal of Computer Trends and Technology, 2012.
30. Nomesh, B., Pranav, S., & Jalaj, B. Quantification of agility of a Supply Chain using Fuzzy Logic. American Journal of Engineering and Applied Sciences: 2 (2), 2012.
31. Common Cybersecurity Vulnerabilities in Industrial Control Systems, Home Land Security, Control Systems Security program, National Cyber security Division, 2011.
32. Max Wandera, Brent Jonasson, Cybersecurity considerations for electrical distribution systems. White Paper WP152002EN, 2014.
33. Common vulnerabilities in critical infrastructure control systems, Sandia National Laboratories Albuquerque, NM 87185-0785, 2nd edition, 2003.
34. Zadeh L. and Kacprzyk J. Computing with Words in Information/Intelligent Systems – Part 1: Foundation; Part 2:

Applications. Heidelberg, Germany: Physica-Verlag, vol.1, 187 – 201, 1991.
35. Breznhev, E. Risk Matrix-Based Method for Critical Infrastructure Safety Assessment Taking into Account Interdependencies [Електронний ресурс] / E. Brezhnev, B. Chernetskiy // Circuits, Systems, Communications and Computers (CSCC): proceedings of XX International Conference, 14-17 July, 2016. - Corfu Island (Greece), 2016. – Режим доступу: http://www.matec-conferences.org/articles/matecconf/pdf/2016/39/matecconf_cscc2
36. 10 CFR 50, Appendix B. Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, US NRC,
37. 10 CFR 73.54, "Protection of digital computer and communication systems and networks", US NRC.
38. Regulatory Guide 1.152, "Criteria for use of computers in safety systems of nuclear power plants", U.S. NRC, 2010.
39. Regulatory Guide 5.71, "Cyber security programs for nuclear facilities", US NRC, 2010.
40. NQA-1a-2009, "Quality Assurance Requirements for Nuclear Facility Applications", ASME, 2009.
41. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE, 2003.
42. IEEE Std 603-1991 "Standard Criteria for Safety Systems for Nuclear Power Generating Stations", IEEE, 1991.
43. DI&C-ISG-01, "Cyber Security Associated with Digital Instrumentation and Controls"
44. DI&C-ISG-06, Revision 1, "Licensing Process", US NRC,
45. IEEE Std 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process", IEEE, 2006.
46. NUREG/CR-7117, "Secure Network Design", US NRC, 2012.
47. NIRMA TG-16, "Software configuration management and quality assurance", NIRMA, 1998.
48. BTP 7-14, "Guidance on Software Reviews on Digital Computer-Based I&C systems", US NRC, 2007.
49. NUREG 6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems", US NRC, 1993.

Литература

АНОТАЦІЯ

УДК 004.9+004.052:621.38

Брежнєв Є.В. **Основи аналізу та забезпечення інформаційної безпеки смарт грид /** За ред. Харченка В.С. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», 2017. – 128 с.

Викладені матеріали практичної частини начального курсу “Аналіз та забезпечення інформаційної безпеки смарт грид” (Smart grid information security analysis and assurance), підготовленого в рамках проекту Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Курс присвячений практиці оцінювання та забезпечення інформаційної безпеки смарт грид, а також їх інформаційно-управляючих систем. Приводиться навчальна програма курсу, опис семінарів, практикумів, тренінгу, методичні рекомендації щодо самостійного вивчення курсу. Даний курс є частиною курсу з “Fundamentals of secure and resilient computing”.

Книга призначена для магістрів, аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів, засобів оцінювання та забезпечення інформаційної безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Бібл. – 49 найменувань, рисунків – 41, таблиць – 26.

ЗМІСТ

Зміст

ABSTRACT

UDC 004.9+004.052:621.38

Brezhnev E. V. Fundamentals of smart grid information security analysis and assurance. Practicum / Edited by Kharchenko V. S. – Kharkiv National Aerospace University named after N. E. Zhukovsky "KhAI", 2017. – 128 p.

ISBN

Practical materials of study course "Fundamentals of smart of grid information security analysis and assurance" given in this book are developed within project Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

The course is devoted to the practical issues of information security risk assessment and assurance of smart grid and their I&C systems. In terms of methodology the following were given: syllabus, description of seminars, practicums, training and recommendations for independent learning of course. This course is part of other course which is devoted to "Fundamentals of secure and resilient computing".

The book is supposed to be used by PhD students of universities that study computer science, computer and program engineering when studying methods and tools for information security assessment and assurance. It could be very useful for lecturers and professors who conduct classes on corresponding courses.

Ref. – 49 items, tables-26, figures – 41.

CONTENT

СОДЕРЖАНИЕ

ПРИЛОЖЕНИЕ. УЧЕБНАЯ ПРОГРАММА

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
Fundamentals of smart grid information security analysis and assurance	**CM4B**

Teacher(s)	Department
Coordinating: Dr. Brezhnev Eugene	Computer Systems and Networks

Study cycle	Level of the module	Type of the module
PhD	A	Full-time tuition

Form of delivery	Duration	Langage(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: – Computer Systems and System Analysis; – Fuzzy Theory Foundations; – FME(C)A Foundations; – Modeling Foundation knowledge and skills.	**Co-requisites (if necessary):**

Credits of the module	Total student workload	Contact hours	Individual work hours
3	90	42	48

Aim of the module (course unit): competences foreseeen by the study programme
The aim of course is to create a knowledge acquisition about software-based tools and methods of smart grid (I&C) information security analysis and modelling. Acquisition of knowledge, engineering methodology on smart grid information security analysis and skills for application and development of software-based tools for practical tasks

related to smart grid security problems' solutions.		
Learning outcomes of module (course unit)	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to: 1. Analyze and evaluate the main features and underlying IT of smart grid. Synthesize information	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
2. Assimilate, evaluate and analyze information related to risk, security analysis of smart grid	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
3. Use fuzzy and matrixes-based methods for security analysis for solving the practical tasks	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
4. Use the software tools for fuzzy security assessment	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
5. Use the tools for systems security analysis	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
6. Analyze the modern smart grid systems in respect to their cyber vulnerabilities	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

Themes	Contact work hours							Time and tasks for individual work	
	Lectures	Consultations	Seminars	Practiacl work	Laboratory work	Placements	Total contact work	Individual work	Tasks
Module 1 METHODS AND TOOLS OF INFORMATION SECURITY ASSESSMENT OF SMART GRID									
1. Introduction to information security of smart grid and I&Cs. New challenges and problems 1.1 Information security from system engineering perspectives: information assurance: confidentiality, integrity, authentication, availability, risk management, threats and vulnerabilities, balancing cost, functionality, and security. 1.2 Information security Risk analysis	2						**2**	6	1.4 Tool support for Secure lifecycle of smart grid components/systems 1.5 Smart grid security measures

foundations. Basic models, measures, criteria. Vulnerabilities, etc. 1.3 Overview of methods for smart grid security assessment									
2.Analysis of methods for smart grid information security risk management 2.1 Smart grid information security risk management: foundations 2.2 Security risk management: methods and tools review. 2.3 Information security incident. Case study methodology	2		4				**6**	6	2.4 Industrial control systems security management 2.5 Review of common security tools: firewalls, access control list, virtual private network, intrusion detection system, and anti-virus, etc.
3. Application of IT for I&C design decisions making support considering information security risks 3.1 Information security requirement	2			4			**6**	4	3.4 Selection of tool support for secure design 3.5 Organization of project security

profiling 3.2 Security risk mitigation framework (who, when and what) 3.3 Assessment of risks during I&C operation									training. Foundations
In total per module	6		4	4			14	16	
Module 2 FUZZY METHODS AND TOOLS FOR INFORMATION SECURITY ASSESSMENT OF SMART GRID									
1.Overview fuzzy approaches for smart grid (I&C) information security analysis 1.1 Foundation of fuzzy sets for security engineering 1.2 Analysis and classification of existing fuzzy methods and approaches for security assessment 1.3 Methods Limitations, peculiarities of application	2						**2**	6	1.4 Soft computing for smart grid security analysis.

2. **Fuzzy extensions for qualitative methods of I&C information security assessment** 2.1 Introduction to Fuzzy event (cyber incidents). 2.2 Operation with fuzzy probabilities and severity. Fuzzy risk values 2.3 Application of fuzzy probabilities for I&C security assessment: Case – study	2			4			**6**	5	2.4 Application of fuzzy risk values for risk mitigation approaches selection
3. Overview of software –based tool for information security and risk fuzzy assessment 3.1 Classification of existing tools for fuzzy security assessment 3.2 Fuzzy logic Software: Taxonomy, Current Research Trends and Prospects 3.3 Case study: application of fuzzy tools for smart grid cyber incident analysis	2			4			**6**	5	3.4 Software for Soft Computing
In total per module	6			8			**14**	16	

Module 3 PROCESS-BASED APPROACHES FOR SMART GRID (I&C) INFORMATION SECURITY ASSURANCE									
1 Analysis of I&C information security standards for safety and reliability related smart grid I&C. 1.1 Potential cyber security threats for SEI 1.2 SEI vulnerabilities classification 1.3 Attack prevention and defense	2			4			**6**	6	1.4 SEI protocol and architecture overview
2. I&C information security assurance measures and methods 2.1 Common vulnerabilities of I&C in smart grid 2.2 Diversity for cyber security assurance 2.3 Project cost effective approaches for I&C security assurance methods selection	2						2	5	2.4 Comparative analysis of SEI security analysis methods
3. Processes-based smart grid I&C information security assurance 3.1 Quality assurance for information security of smart grid. 3.2 QA supports of	2			4			**6**	5	3.4 Advanced metering infrastructure security

information security life cycle 3.3 NQA vise ISO: information security aspects									
In total	6			8			14	16	
Total/per course	18		4	20			42	48	

Assessment strategy	**Weight in %**	**Dead lines**	**Assessment criteria**
Lecture activity, including fulfilling special self-tasks	10	7,14	**85% – 100%** Outstanding work, showing a full grasp of all the questions answered. **70% – 84%** Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. **60% – 69%** A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. **50% – 59%** There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. **45% – 49%** Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others

			will be either omitted or incorrect. **40% – 44%** There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. **20% – 39%** There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. **0% – 19%** Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	**85% – 100%** An outstanding piece of work, superbly organized and presented, excellent achievement of the objectives, evidence of original thought. **70% – 84%** Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organization and presentation. **60% – 69%** Students will show a clear understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. **50% – 59%** The work should show evidence that the student has a

			reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organization should be reasonably clear, and the objectives should at least be partially achieved. **45% – 49%** Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. **40% – 44%** There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. **20% – 39%** The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. **0% – 19%** Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Module Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of periodical or volume	Place of printing. Printing house or internet link
Compulsory literature				
Brezhniev E., Kovalenko A. Illiashenko O.	2016	Assurance of cyber security for I&C systems important to safety: process approach based on quality management system	-	Proceeding of 10th International Conference "DEpendable Systems, SERvices and Technologies" (DESSERT 2016). – Kiev, Ukraine.
Netkachov, O., Popov, P. and Salako, K.	2016	Model-based evaluation of the resilience of critical infrastructures under cyber attacks.	vol 8985.	Lecture Notes in Computer Science, Springer, Cham
Bloom Field, R., Bendele, M., Bishop, P., Stroud, R. and Tonks, S.	2016	The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned.	-	Proceedings of the First International Conference, RSSRail 2016, 28-2016, Paris, France.
Kharchenko V.,	2015	Secure Hybrid Clouds:	Vol.365 . –	Springer International

Ponochovny Y., Boyarchuk A., Gorbenko A.		Analysis of Configurations Energy Efficiency	Pp.195 –209.	Publishing Switzerland
Коваленко А.В.	2015	Обеспечение информационной безопасности ИУС АЭС	-	Проблеми інформатизації. Матеріали четвертої міжнародної НТК. – Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ.
Popov, P.T., Netkachov, A. and Salako, K.	2014	Quantification of the Impact of Cyber Attack in Critical Infrastructure.	-	Proceedings of SAFECOMP 2014 Workshops: ReSA4CI 9 September, Florence, Italy.
Al-Sudani Mustafa Qahtan Abdulmunem, Kharchenko V.S., Uzun D.D.	2015	Vulnerability analysis of wireless networks: case for smart building automation	№2(72) . – С. 69–76.	Радіоелектронні і комп'ютерні системи. – Харків: НАКУ «ХАИ»
Б.М. Конорев, И.Б. Туркин, В.В. Сергиенко, В.С. Харченко, Г.Н. Жолткевич, В.О. Мищенко,	2012	Инженерия критического программного обеспечения	Volume 28, number 1	Харьков: Нац. аэрокосм, ун-т им. Н.Е. Жуковского «Харьк. авиац. ин-т»

А.А. Гордеев				
Харченко В.С., Поночовный Ю.Л., Фурманов А.А., Васильев К.А.	2015	Модели развития уязвимостей IT-продуктов: патологические цепочки в контексте марковского анализа	Вип. 12 (137). – С. 114–119.	Системи обробки інформації
V. Kharchenko, E. Brezhnev	2015	Smart Grid Substation Availability Assessment: Recovered MSS-Based Approach	-	ESREL 2015 25th European Safety and Reliability Conference / Proceeding of the 25th European Safety and Reliability Conference
V. Kharchenko, E. Brezhnev	2015	Cyber diversity for digital substations under uncertainties: assurance and assessment/	-	Proceedings of CSCC / INASE, Zakynthos Island /Recent Advances in Computer Science, ISBN: 978-1-61804-320-7
Additional literature				
Shujun Xin, et.al.	2017	Information Masking Theory for Data Protection in Future Cloud-based Energy Management	Volume PP Issue 99	IEEE Transactions on Smart Grid

C. Lopez, et.al.	2015	Smart Grid Cyber Security: An Overview of Threats and Countermeasures	#9	Journal of Energy and Power Engineering
S.Goel, et.al.	2015	Smart Grid Security	-	Springer International Publishing Switzerland
F. Skopik, P. Smith	2015	Smart Grid Security: Innovative Solutions for a Modernized Grid 1st Edition	-	Elsevier, Inc
A.Bari	2014	Challenges in the Smart Grid Applications: An Overview	1	International Journal of Distributed Server Networks
L. Zadeh	1965	Fuzzy sets	Vol. 8.	Inf. Control.

Брежнєв Євген Віталійович

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГЕТИЧНИХ ІНФРАСТРУКТУР

Практикум

(російською мовою)

Редактор Харченко В.С.

Комп'ютерна верстка
Л.Д. Харченко

Зв. план, 2012
Підписаний до друку 03.04.2017
Формат 60x84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 71,76. Уч.-вид. л. 73,52. Наклад 100 прим.
Замовлення 42. Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu

Віддруковано ФОП Лисенко І.Б.
61070, Харків-70, вул. Чкалова, 17, моторний корпус, к. 147
Свідоцтво про внесення суб'єкта видавничої справи в державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції
ДК №2607 от 11.09.06 р.