iGrids
интеллектуальные сети

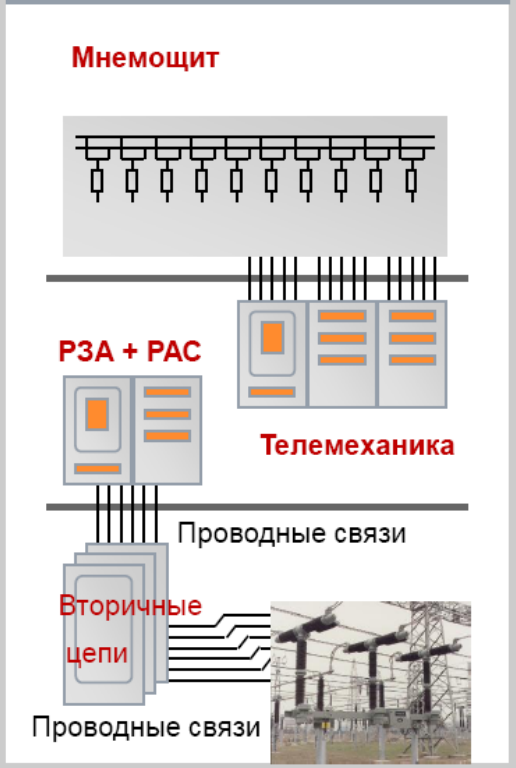
Требования к программному обеспечению терминалов релейной защиты на основе МЭК 15408

Перспективы и проблемы применения

Максим Никандров
к.т.н., директор компании iGrids
ООО «Интеллектуальные Сети»

Эволюция систем управления энергообъектом

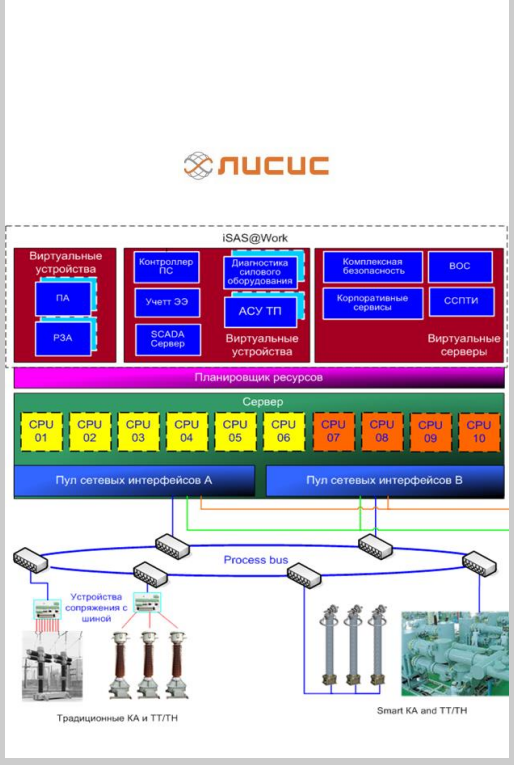
Первое поколение:
Традиционная телемеханика
до 1986



Второе поколение:
Микропроцессорные ПС
с 1986 г

Третье поколение:
Цифровые ПС
с 2004 г

Четвертое поколение:
Цифровые ПС (виртуальные РЗА)
с 2015 г



iGrids интеллектуальные сети

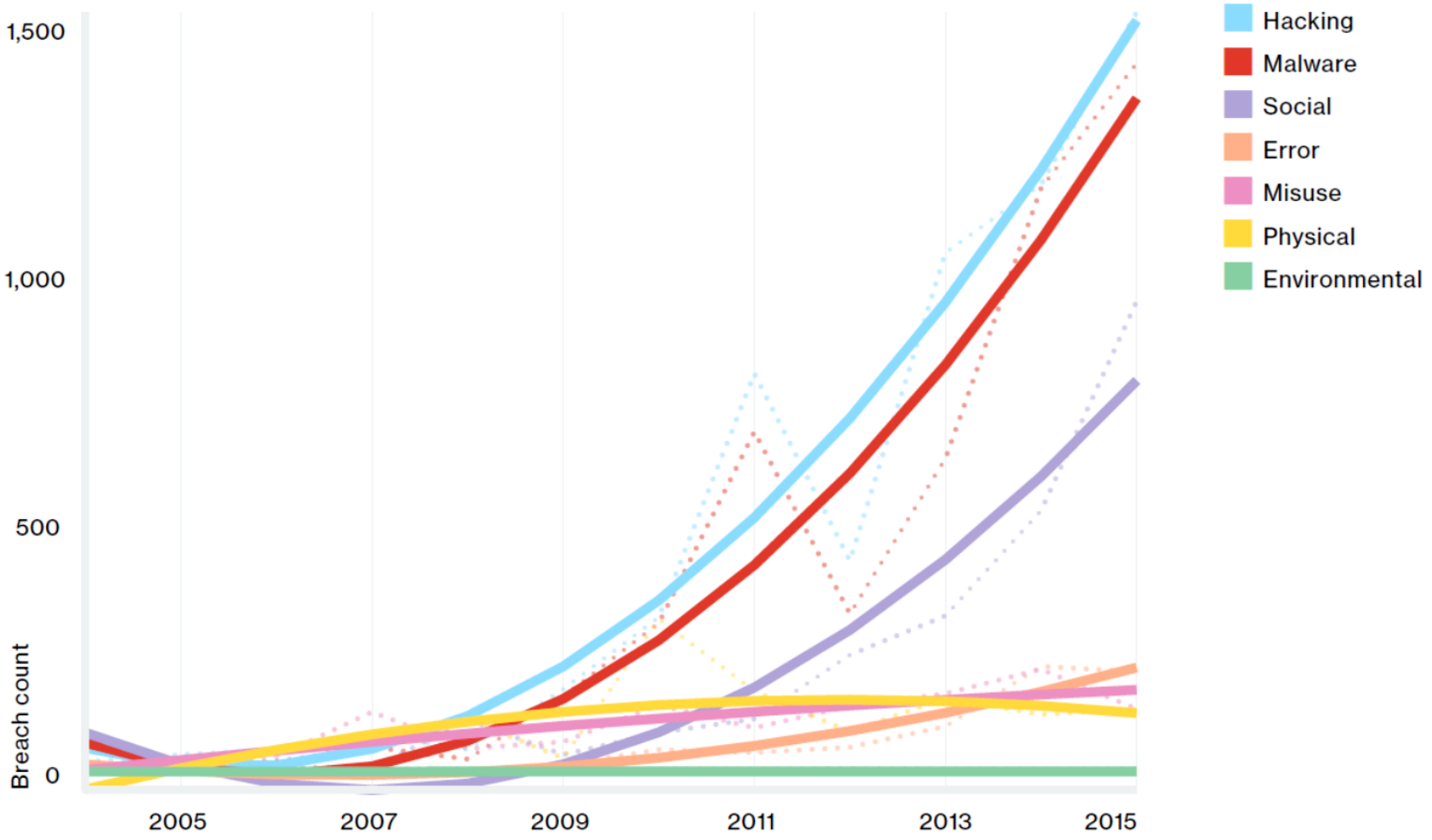
Изменение стоимости и влияния ПО

						
Описание	Электромеханические реле	Полупроводниковые панели	Микропроцессорные РЗА	Микропроцессорные РЗА со специализированной ОС (VxWorks)	Компьютерные РЗА под управление Linux и других ОС	Виртуальные РЗА (программные модули)
Стоимость ПО* (% от общей стоимости)	**0 %**	**0 %**	**35 %**	**45 %**	**75 %**	**90 %**

*экспертная оценка

iGrids интеллектуальные сети

Изменение причин, приведших к инцидентам в АСУ ТП



Отчет Verizon Data Breach Digest 2017

iGrids интеллектуальные сети

Проверка на недекларируемые возможности

1

Контроль отсутствия недекларированных возможностей

- **НДВ -** функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

- **Программные закладки -** преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

iGrids интеллектуальные сети

Необходимые политики безопасности объекта

2

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-2-2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 2.

Функциональные компоненты безопасности

ISO/IEC 15408-2:2008
Information technology–Security techniques–
Evaluation criteria for IT security–Part 2. Security functional components
(IDT)

iGrids интеллектуальные сети

Необходимые политики безопасности объекта

2

P.DENY_UNAU **Защита от несанкционированного доступа**

Должно обеспечиваться предотвращение несанкционированного доступа к информации.

P.IDENT_ASSET **Идентификация и инвентаризация активов**

Должно обеспечиваться выявление незарегистрированных и несанкционированных технических устройств, и программных средств, которые могут привести к нарушению работы программного обеспечения.

P.AUDIT **Контроль обеспечения информационной безопасности**

Должен осуществляться контроль за действиями пользователей ОО и за событиями безопасности, связанными с ОО.

P.ACC_MON **Разграничение доступа**

Должно осуществляться разграничение доступа пользователей ОО к активам.

P.SECURE **Защита критической информации**

Должна осуществляться защита критически важной технологической информации на всех этапах ее жизненного цикла.

iGrids интеллектуальные сети

Документы по оценочному уровню доверия

3

НАЦИОНАЛЬНЫМ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТР 56939 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

iGrids интеллектуальные сети

Документы по оценочному уровню доверия

3

1. Разработка и сборка ПО

Перечень инструментальных средств разработки ПО

Разработчику ПО следует использовать последние доступные версии инструментальных средств и их возможности по проверке создаваемой программы на наличие проблем

Порядок оформления исходного кода программы

Создать (выбрать) и использовать при создании программы порядок оформления исходного кода программы, содержащий перечень правил и рекомендаций, направленных на устранение недостатков программы (потенциально уязвимых конструкций) в исходном коде программы.

Регламент и протоколы статического тестирования программы

Периодический потенциально уязвимых конструкций в исходном коде программы (при выявлении)описание действий, направленных на их устранение, или обоснование невозможности или отсутствия необходимости в доработке программы

Регламент и протоколы экспертизы исходного кода программы

Экспертизу исходного кода программы выполняет разработчик ПО, обладающий компетенцией в области выявления уязвимостей программы, для актуальной версии исходного кода программы. Выполнение экспертизы исходного кода программы непосредственно создателями исходного кода программы (программистами) нежелательно.

iGrids интеллектуальные сети

Документы по оценочному уровню доверия

3

2. Тестирование ПО

Регламент и протоколы функционального тестирования

Функциональное тестирование программы для того, чтобы определить, выполняются ли требования безопасности
Для эффективного тестирования рекомендуется разделять между специалистами обязанности по созданию программы и ее функциональному тестированию.

Регламент и протоколы тестирования на проникновение

Проведение тестирования на проникновение в отношении программы с целью выявления ее уязвимостей.
Тестирование на проникновение предполагает выявление уязвимостей программы путем моделирования (имитации) действий потенциального нарушителя. Тестирование на проникновение выполняют сторонние организации, обладающие компетенцией в области проведения такого рода испытаний, для актуальной версии программы. Выполнение тестирования на проникновение непосредственно разработчиками или специалистами по функциональному тестированию программы нежелательно.

Регламент и протоколы динамического анализа кода программы

Анализ осуществляется во время работы программы с целью обнаружения в них дефектов различного рода при помощи целенаправленной генерации входных данных.

Регламент и протоколы фазинг тестирования

Техника тестирования программного обеспечения, часто автоматическая или полуавтоматическая, заключающая в передаче приложению на вход неправильных, неожиданных или случайных данных. Предметом интереса являются падения и зависания, нарушения внутренней логики и проверок в коде приложения, утечки памяти, вызванные такими данными на входе.

iGrids интеллектуальные сети

Документы по оценочному уровню доверия

3

3. Управление инфраструктурой среды разработки ПО

Регламент защиты инфраструктуры среды разработки ПО

Определить элементы конфигурации, имеющие отношение к разрабатываемому ПО, которые должны быть защищены от угроз безопасности информации, связанных с нарушением конфиденциальности, целостности и доступности. Разработчик ПО должен применять технические и организационные меры, обеспечивающие защиту от несанкционированного доступа определенным элементам конфигурации

Регламент резервного копирования конфигурации ПО

Определить подлежащие резервному копированию элементы конфигурации, имеющие отношение к разрабатываемому ПО. Разработчик ПО должен применять технические и организационные меры, обеспечивающие резервное копирование и восстановление определенных элементов конфигурации с периодичностью, определенной в документации разработчика ПО.

Регламент регистрации событий изменений конфигурации ПО

Применять технические и организационные меры, обеспечивающие регистрацию всех событий, связанных с фактами изменения элементов конфигурации, в журналах регистрации событий. Следует регистрировать следующую информацию: инициатор изменения, идентификатор элемента конфигурации, дата и время изменения элемента конфигурации.

Журнал регистрации изменений конфигурации ПО

iGrids интеллектуальные сети

4. Управление документацией и конфигурацией ПО

Регламент защиты инфраструктуры среды разработки ПО

Определить элементы конфигурации, имеющие отношение к разрабатываемому ПО, которые должны быть защищены от угроз безопасности информации, связанных с нарушением конфиденциальности, целостности и доступности. Разработчик ПО должен применять технические и организационные меры, обеспечивающие защиту от несанкционированного доступа определенным элементам конфигурации

Регламент резервного копирования конфигурации ПО

Определить подлежащие резервному копированию элементы конфигурации, имеющие отношение к разрабатываемому ПО. Разработчик ПО должен применять технические и организационные меры, обеспечивающие резервное копирование и восстановление определенных элементов конфигурации с периодичностью, определенной в документации разработчика ПО.

Регламент регистрации событий изменений конфигурации ПО

Применять технические и организационные меры, обеспечивающие регистрацию всех событий, связанных с фактами изменения элементов конфигурации, в журналах регистрации событий. Следует регистрировать следующую информацию: инициатор изменения, идентификатор элемента конфигурации, дата и время изменения элемента конфигурации.

Журнал регистрации изменений конфигурации среды разработки ПО

Регламент управления конфигурацией ПО

Разработчик ПО должен использовать систему управления конфигурацией ПО. позволяющую уникально идентифицировать определенные элементы конфигурации.

iGrids интеллектуальные сети

Документы по оценочному уровню доверия

3

4. Решении проблем в ПО в процессе эксплуатации

Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы Процедура устранения ошибок ПО и уязвимостей программы должна обеспечивать прием и обработку сообщений от пользователей об ошибках ПО и уязвимостях программы и запросов на их устранение
Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы Документация разработчика ПО должна содержать описание методов приема и обработки сообщений от пользователей в ситуациях, когда неизвестная ранее уязвимость программы используется для проведения компьютерной или сетевой атаки
Регламент экстренного выпуска обновлений ПО В экстренных ситуациях разработчик ПО должен быть способен к выпуску обновлений ПО в обход стандартной процедуры выпуска новых версий ПО. Если экстренный выпуск обновлений ПО невозможен, разработчик ПО должен предложить альтернативные способы временного решения проблемы, включая использование пользователем дополнительных средств защиты.
Регламент доведения до пользователей информации об уязвимости программы и рекомендаций по их устранению Разработчик ПО должен обеспечить доведение до пользователей информации об уязвимостях программы и рекомендаций по их устранению, в том числе путем обновления ПО.
Журнал ошибок и уязвимостей программы

iGrids интеллектуальные сети

Проблемы

1. Катастрофически не хватает специалистов в области безопасной разработки ПО и осведомлённости среди программистов;

2. Имеющиеся профили защиты для ОС не подходят для ПО РЗА

Выводы

1. Законодательная и нормативная база для требований к ПО РЗА готовы.

2. Требования предъявляются не только к самому программному обеспечению, но и к документации, технологии производства и тиражирования;

3. Применение данных требований может реально повысить качество ПО с точки зрения ИБ и эффективность разработки ПО.

iGrids интеллектуальные сети

Спасибо за внимание!

Максим Никандров
ООО «Интеллектуальные Сети»
nikandrov@igrids.ru