ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ “МЭИ”
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Защищенная ОС на базе Linux и крипто-защищенные протоколы GOOSE и MMS: результаты исследований.

Волошин Александр Александрович
К.т.н, доцент
Почетный доктор электротехники,
Чл.-корр. АЭН РФ

Директор Центра НТИ
«Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем»
НИУ «МЭИ»

КИБЕРУЧЕНИЯ НАТО

- Киберучения НАТО «Locked Shields»
- Организуются и проводятся Центром передового опыта по совместной защите от киберугроз с 2010 года.
- Киберучения НАТО «CyberCoalition»

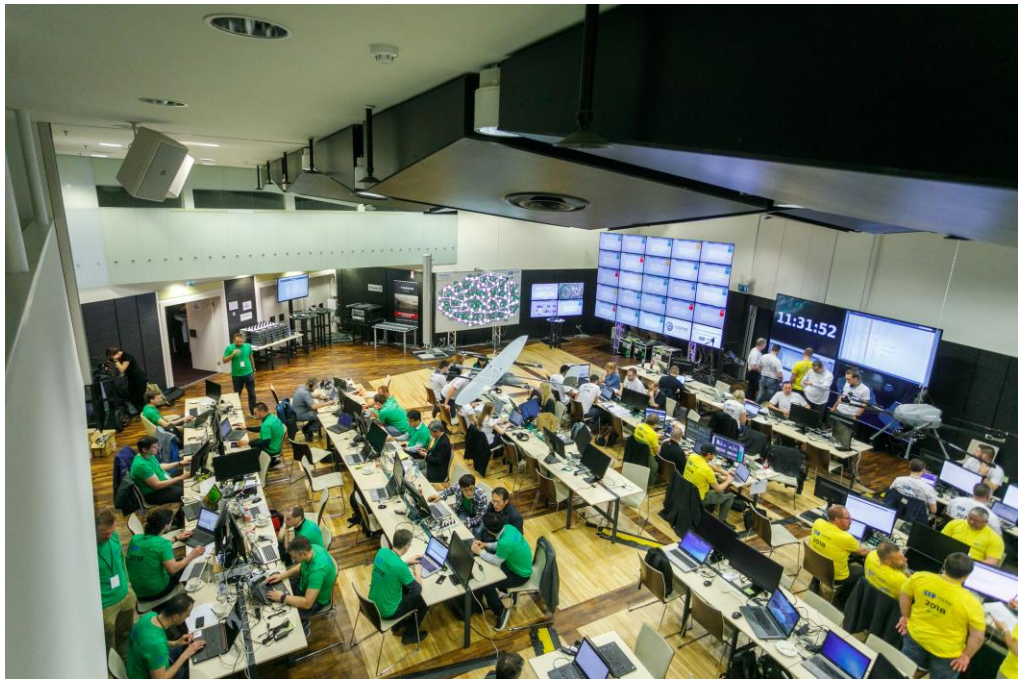
Организуются и проводятся Центром передового опыта по совместной защите от киберугроз (CCDCOE) с 2006 года.

В рамках киберучений имитируются сценарии массированных кибератак на объекты критической инфраструктуры государства или ряда государств.

КИБЕРУЧЕНИЯ НАТО

CCDCOE ежегодно с 2010 года организует мероприятие, позволяющее экспертам по кибербезопасности повысить свои навыки :

- защиты национальных систем ИТ
- защиты критически важной инфраструктуры в условиях атак в режиме реального времени.



Основное внимание уделяется реалистичным сценариям, передовым технологиям и моделированию сложных масштабных киберинцидентов, реагирование на которые требуют принятие стратегических решений, учитывать юридические и коммуникационные аспекты (PR).

КИБЕРУЧЕНИЯ НАТО LOCKED SHIELDS 2023

38 стран участниц

Более 3000 участников

Red Team vs Blue Team training exercise

Более 5500 виртуальных объектов

https://ccdcoe.org/exercises/locked-shields/

Новое требование к РЗА

Устойчивость функционирования защищаемого объекта

– это способность объекта сохранять свои основные функции с заданным качеством (в заданных пределах) под воздействием деструктивных факторов (в частности, под воздействием компьютерных атак)

МЕХАНИЗМЫ И ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

ДОВЕРИЕ

- Российские CPU и MCU
- Доверенные операционные системы
- Доверенная загрузка устройства
- Доверенные обновления
- Удаленная аттестация устройства

АУТЕНТИФИКАЦИЯ

- Устройства
- Пользователя
- Обеспечение неотказуемости для данных, передаваемых устройством

СЕТЕВАЯ БЕЗОПАСНОСТЬ

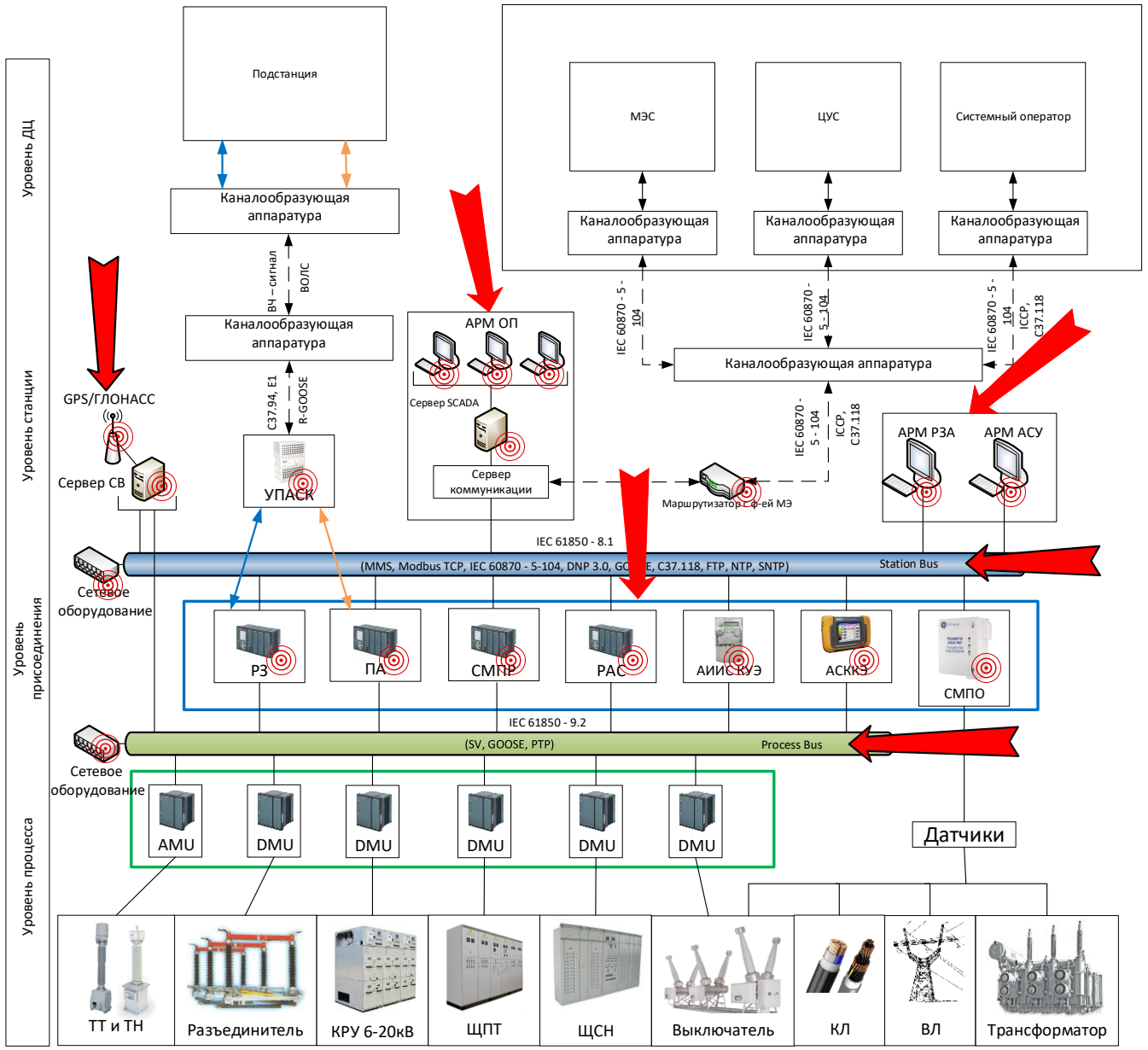
- Встроенный МЭ
- Криптографически защищенные протоколы обмена (MMS, GOOSE, МЭК 60870-5-104)

МЕХАНИЗМЫ БЕЗОПАСНОСТИ

- Встроенный МЭ
- Логирование событий
- Контроль целостности ПО устройства
- Мониторинг и обнаружение атак

Карантаев В. Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий //
Круглый стол НИК D2 РНК СИГРЭ на IX Международной научно-практической конференции «Автоматизация и информационные технологии в энергетике» (Москва, 2019)

Модель угроз ЦПС



Виды возможных атак

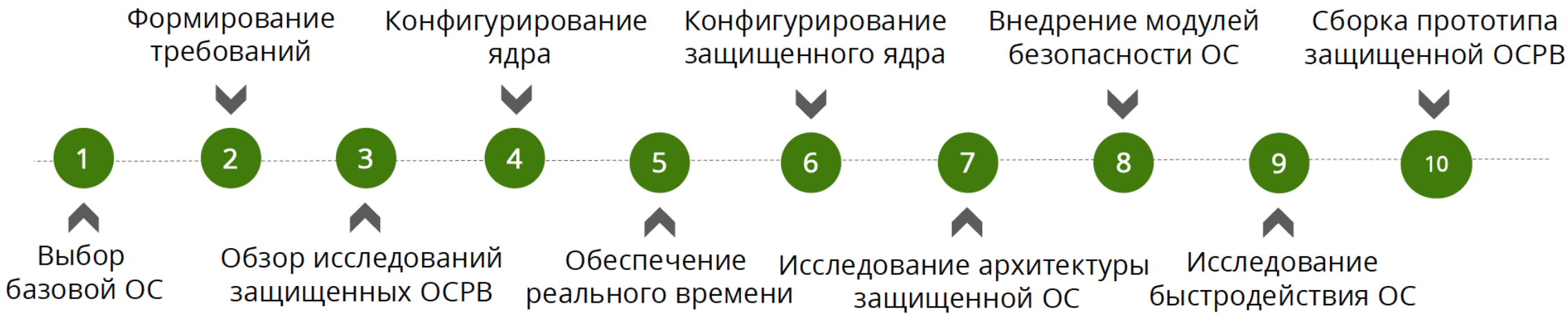
- GPS/ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом

кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, цифровым сетям)

Атаки на устройства

Атаки на протоколы

Операционная система для РЗА



Большой вызов: Real-Time + встроенные механизмы безопасности!

Формирование требований к SDK

Компонент	Версия	Обоснование выбора
Ядро	5.10	LTS версия ядра, поддерживаемая Технологическим центром исследования безопасности ядра Linux
Yocto	4.0	Ведущие разработчики встраиваемых ОС, при выборе ядра версии 5.10 ориентируются на данную версию Yocto
Библиотека GUI-фреймворка QT	5.15.2	Ведущие разработчики встраиваемых ОС, при выборе ядра версии 5.10 ориентируются на данную версию QT
Системная библиотека glibc	2.33	Максимальная LTS версия, поддерживая QT 5.15.2
Компилятор gcc	10.2	Максимальная стабильная версия, поддерживаемая ядром 5.10 и QT 5.15.2
Отладчик gdb	10.2	Максимальная стабильная версия, поддерживаемая ядром 5.10 и QT 5.15.2
Утилита автоматизации процесса компиляции make	4.3	Стабильная версия, совместимая с gcc 10.2, gdb 10.2
Набор программ сборки объектных файлов binutils	2.36	Стабильная версия, совместимая с gcc 10.2, gdb 10.2 и make 4.3
Java	Liberica JDK 8	Отечественная JDK, совместимая с фреймворком для создания мультиагентных систем (Jade)
RTPatch	PREEMPT RT 5.10	Напрямую зависит от версии ядра Linux.

Архитектура защищенной ОС

Монитор обращений — абстрактная сущность, которая осуществляет политику управления доступом объекта. Он проверяет, что субъекты имеют необходимые права доступа, защищая объекты от несанкционированного доступа и изменения.

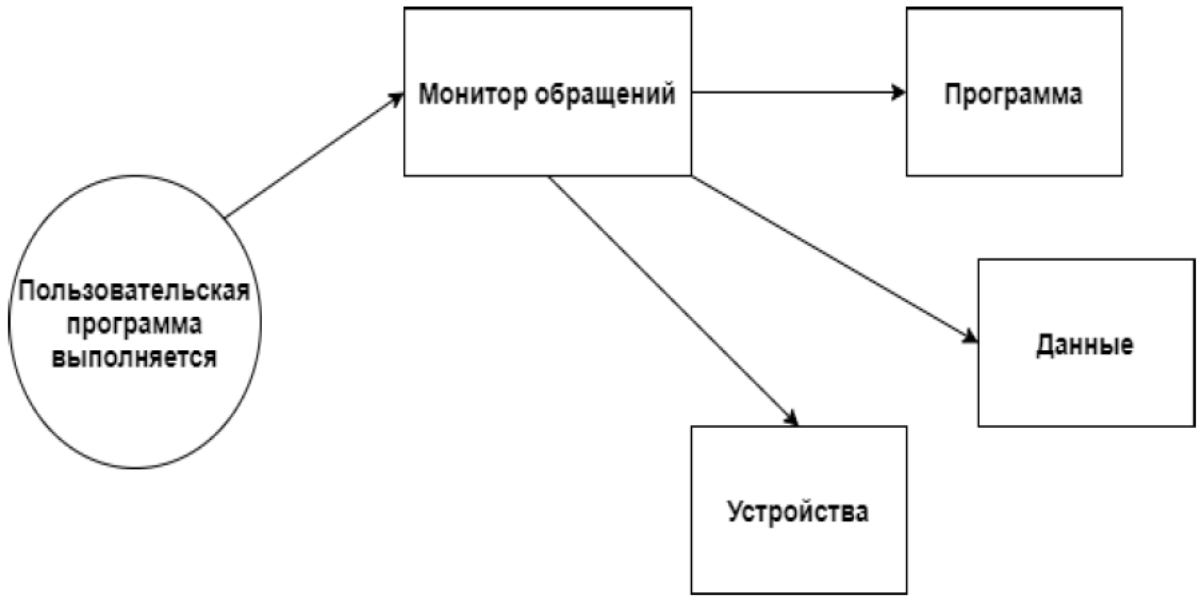
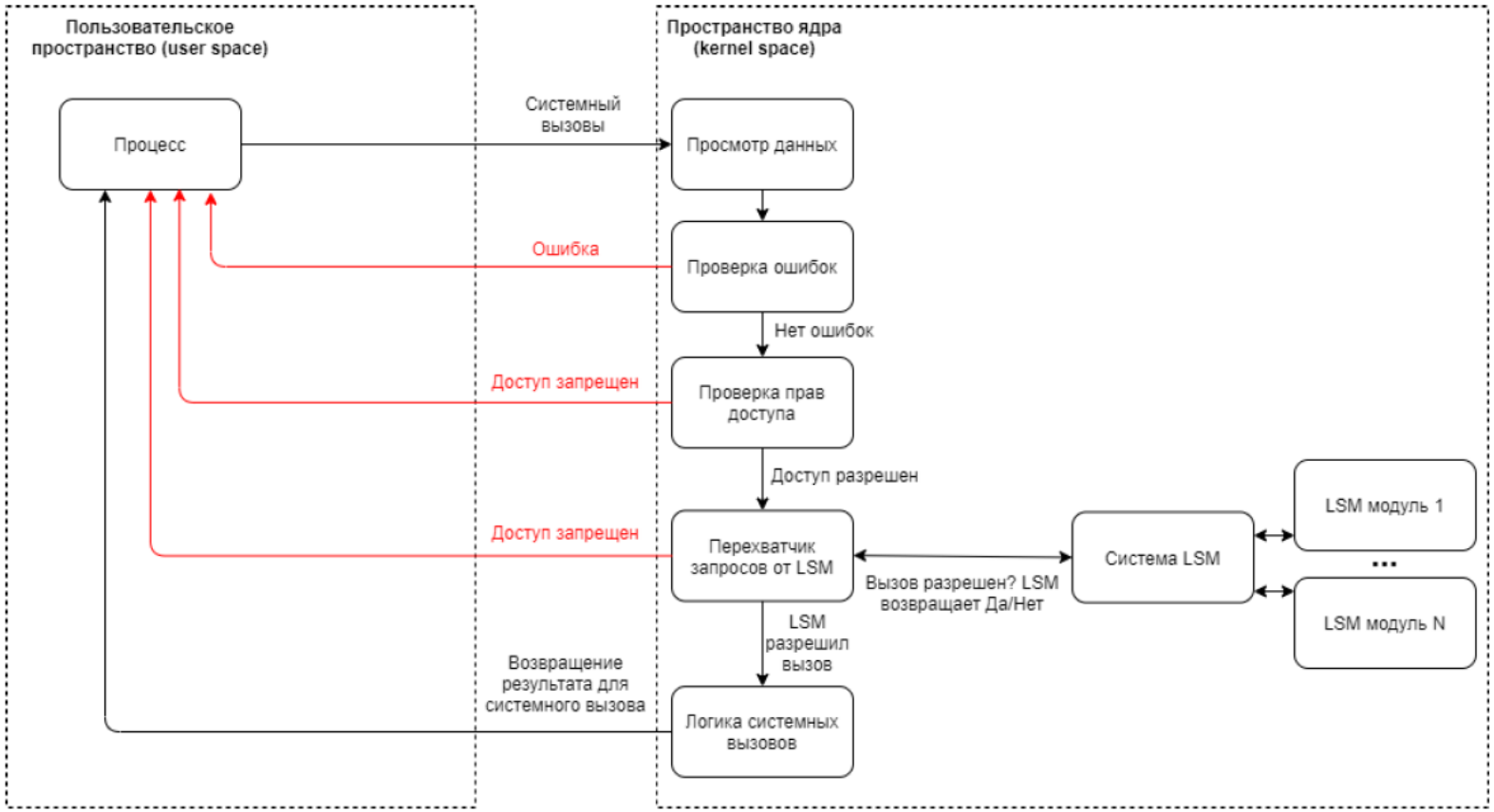


Схема работы монитора обращений в общем виде

Модули безопасности Linux

- Одна из первых реализаций FLASK — SELinux, один из ключевых **модулей безопасности (LSM)**.
- Требующей изучения является **совместимость различных LSM друг с другом**.



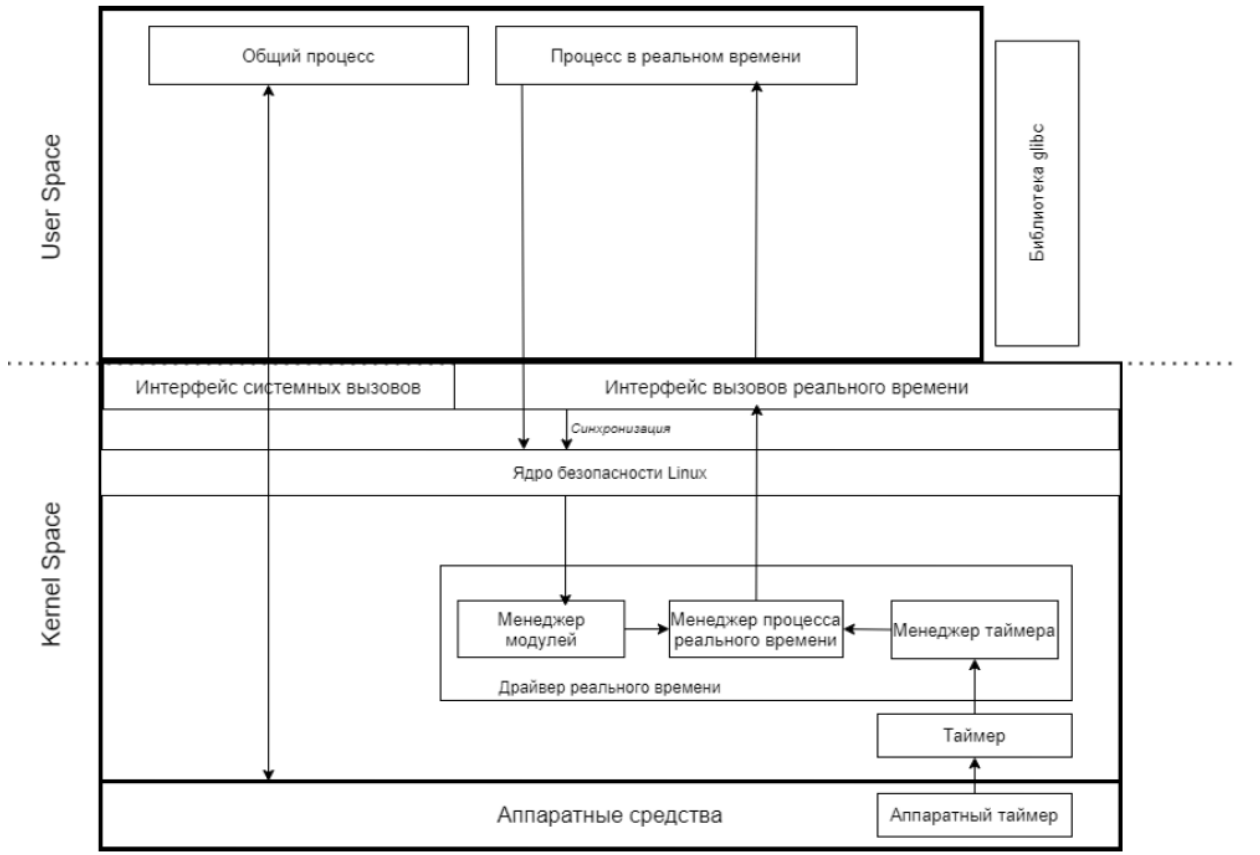
Модули безопасности Linux

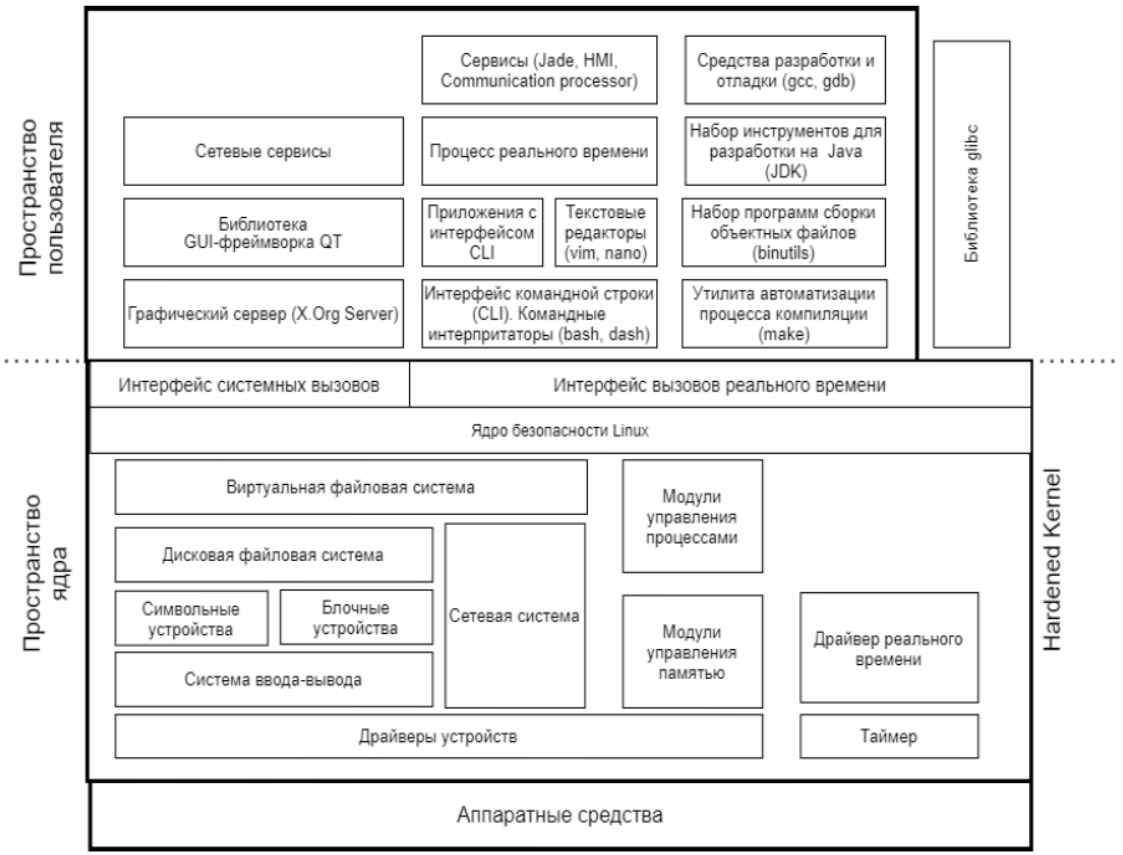
SELinux не единственная реализаций LSM. Существует еще несколько реализаций, самые известные из них:

- AppArmor — система мандатного контроля доступа, в которой большое внимание уделяется защите на уровне приложений, основанной преимущественно на путях файловой системы.
- Smack — система мандатного контроля доступа, использующая метки для процессов и ресурсов. Метки содержат идентификаторы безопасности, которые Smack интерпретирует для обеспечения контроля доступа, требуя меньшего количества правил, нежели SELinux.
- TOMOYO — система мандатного контроля доступа. Она автоматически создает политики на основе поведения приложений, как и AppArmor, её политики в основном используют пути, а не метки.
- LoadPin — модуль, обеспечивающий загрузку всех ресурсов ядра Linux (таких как модули ядра и встроенное ПО) из единой файловой системы, недоступной для записи.
- Yama — модуль, добавляющий дополнительные элементы управления доступом к действиям, которые недостаточно детализированы.
- SafeSetId — модуль, позволяющий более точно контролировать, какие пользователи могут использовать setuid (переключение на другого пользователя). Вместо того, чтобы разрешать использование setuid, SafeSetId может ограничить эту возможность для ряда пользователей.
- Lockdown — модуль, защищающий память ядра Linux. Имеет два режима: в режиме целостности он предотвращает изменение объектов ядра из пользовательского пространства; в режиме конфиденциальности он дополнительно предотвращает извлечение потенциально конфиденциальной информации из ядра.

Модуль Capability по умолчанию включен в системах и обеспечивает поддержку возможностей Linux (набор разрешений, предоставляемых пользователю, когда ему назначены определенные возможности).

Внедрение модулей безопасности в ядро ОСРВ

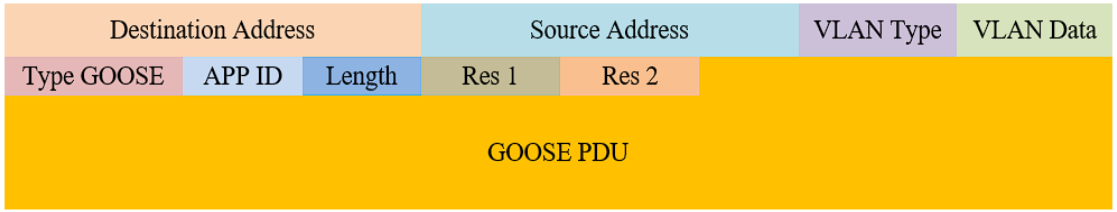




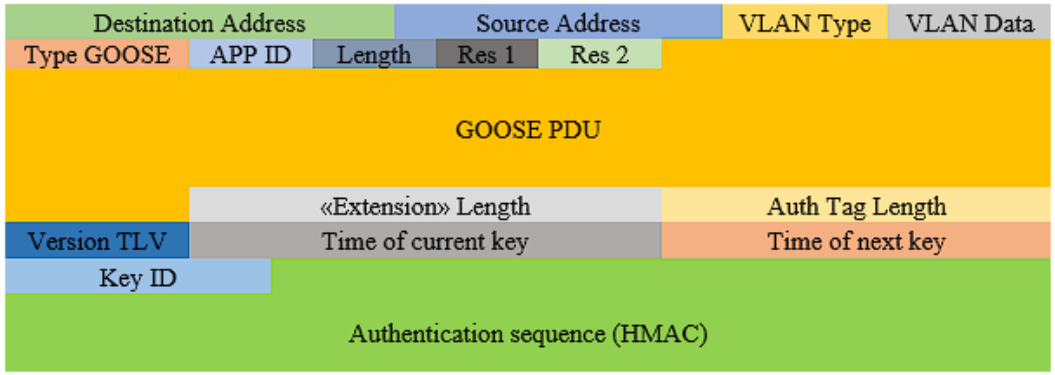
Удалось внедрить модули безопасности в ядро Linux и обеспечить при этом Real-Time!

Криптозащищенный GOOSE

Обычный



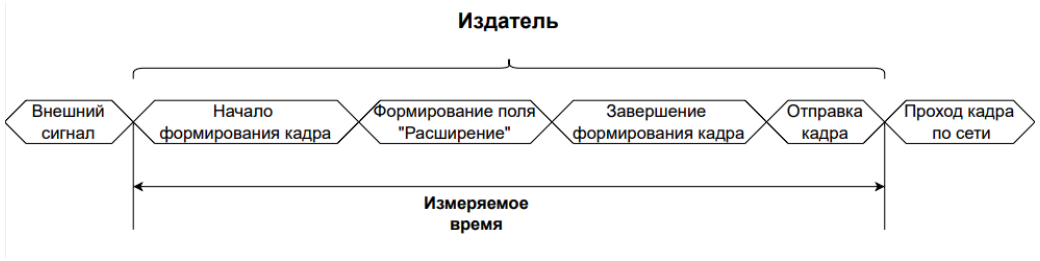
Криптозащищенный

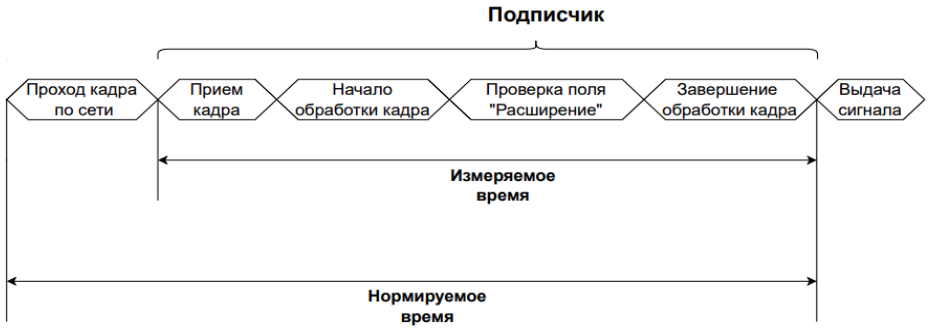


Структура GOOSE сообщения согласно МЭК 62351-6

В ходе проведения испытаний использовались хеш-функции HMAC-SHA256 и HMAC-SHA512 из состава программной библиотеки libssl-dev 3.0.9-1.

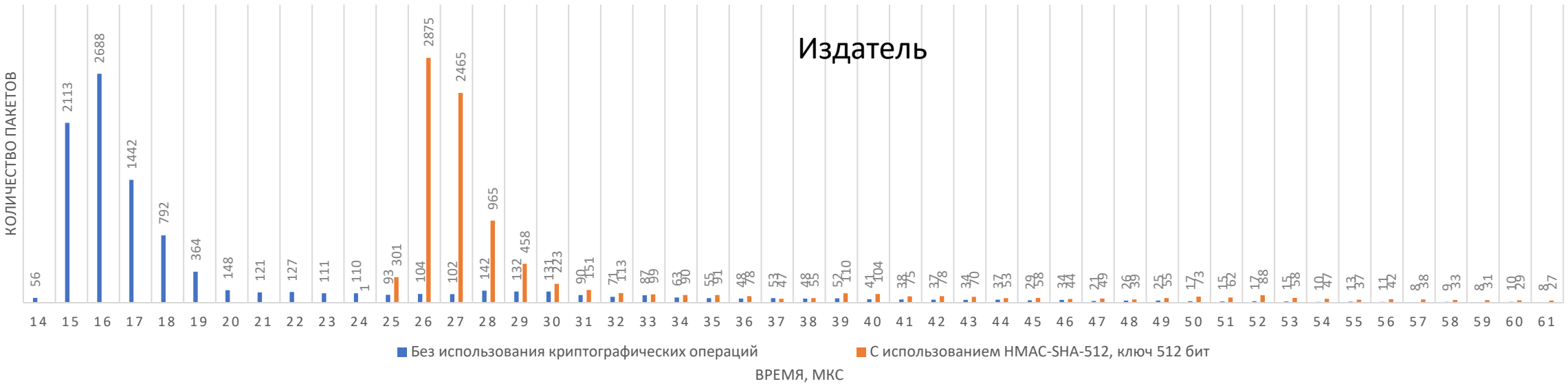
Криптозащищенный GOOSE

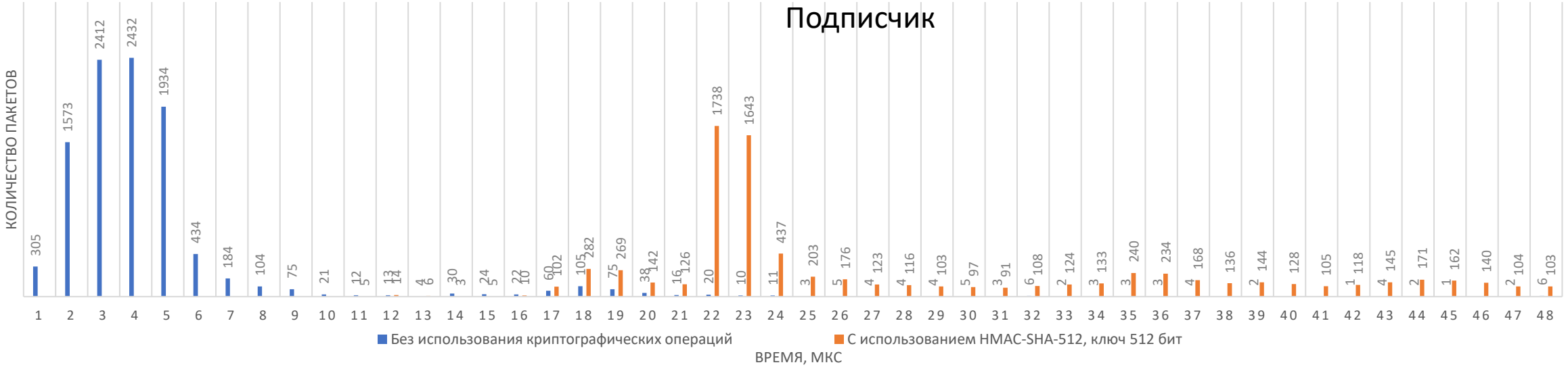




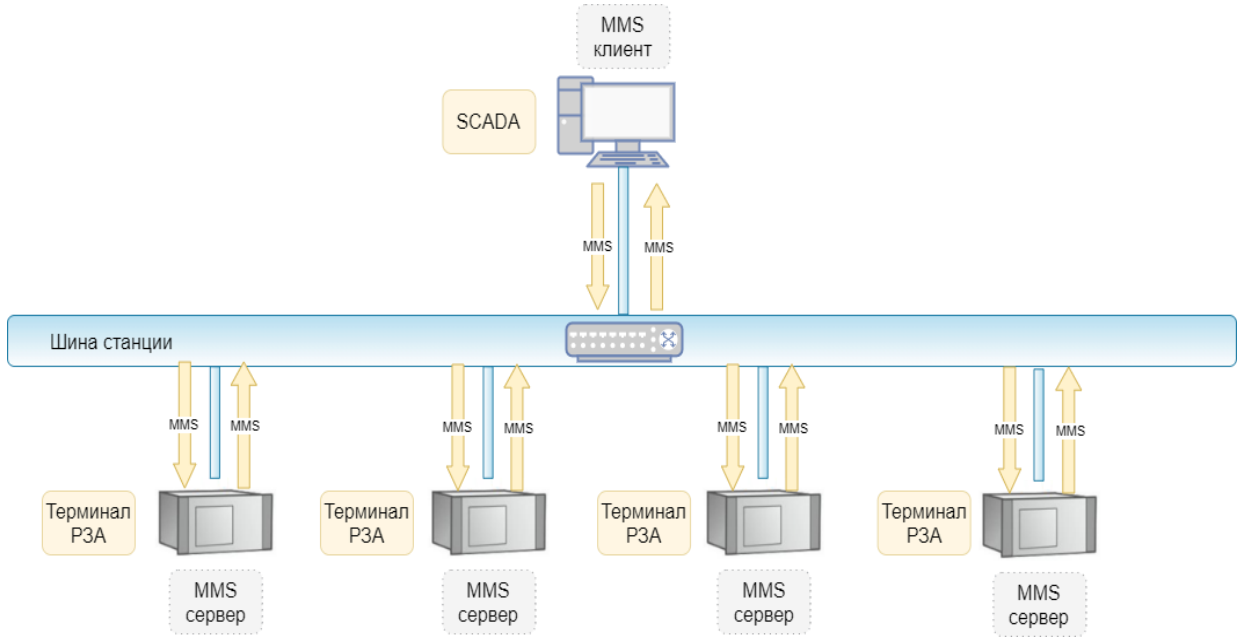
Алгоритм	Размер пакета, байт	Размер ключа, бит	Издатель			Подписчик		
			Макс. время, мкс	Мин. время, мкс	Мед. время, мкс	Макс. время, мкс	Мин. время, мкс	Мед. время, мкс
Без криптографии	189	-	255	11	13	76	1	1
	549	-	295	12	14	168	1	3
	1416	-	182	14	17	310	1	3
HMAC-SHA256	189	128	574	20	22	512	5	16
	549	128	231	21	24	187	7	18
	1416	128	203	25	29	211	11	23
	189	256	512	19	22	195	5	16
	549	256	174	21	24	336	6	19
	1416	256	355	25	28	267	11	23
	189	512	245	19	22	438	5	17
	549	512	322	22	25	335	6	18
	1416	512	297	25	28	661	11	26
HMAC-SHA512	189	128	168	19	23	381	6	19
	549	128	187	21	24	278	8	21
	1416	128	472	25	28	339	11	26
	189	256	367	19	22	209	5	19
	549	256	263	22	25	404	7	23
	1416	256	252	25	28	323	11	26
	189	512	467	19	22	340	5	20
	549	512	553	22	25	204	7	22
	1416	512	716	24	28	734	11	26

Криптозащищенный GOOSE

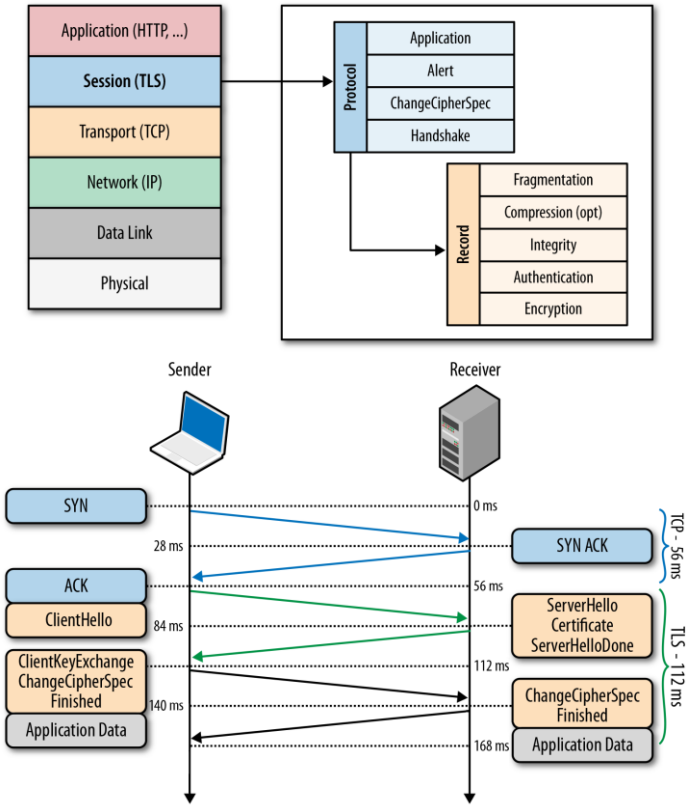




Криптозащищенный MMS

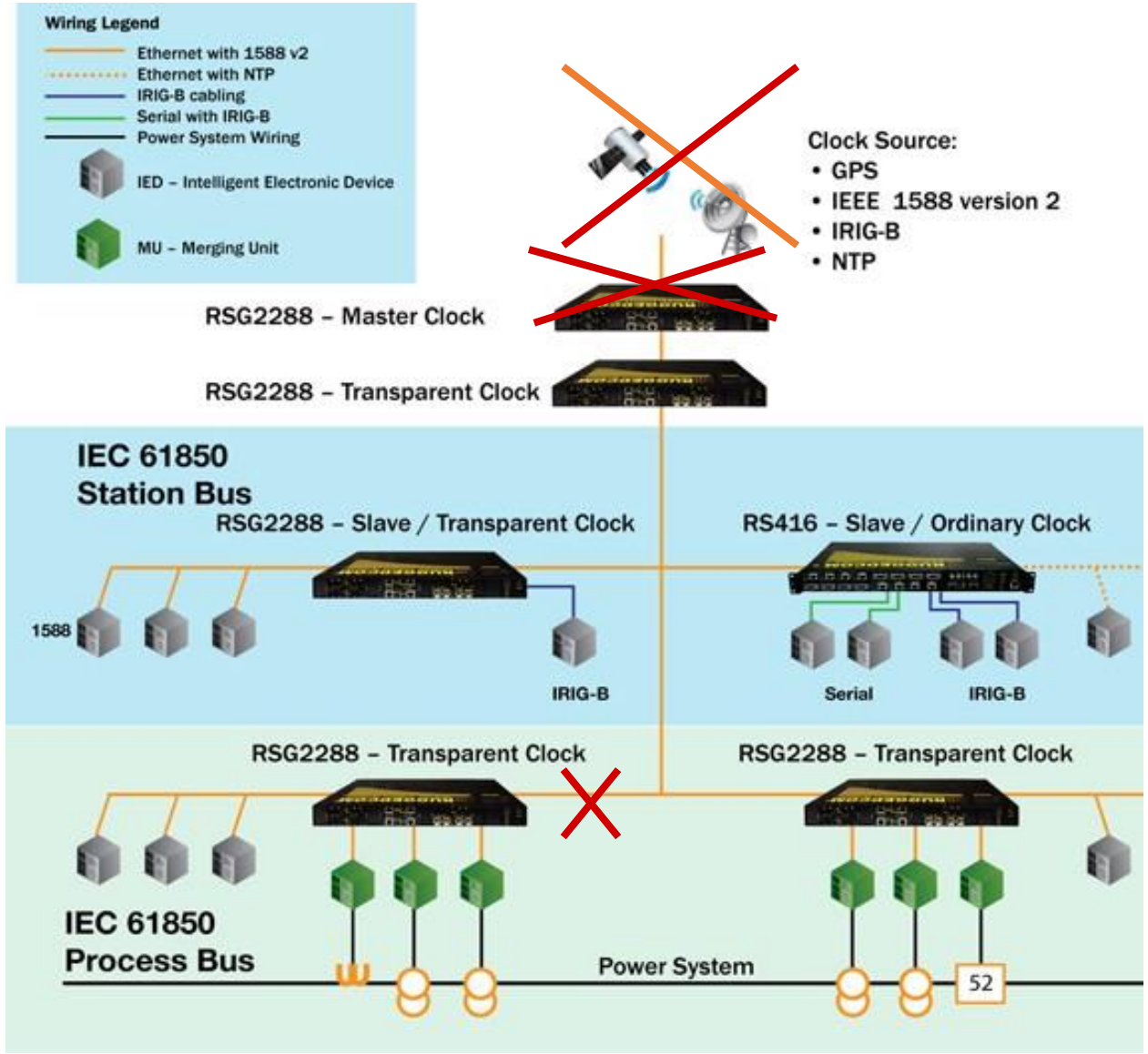


Протокол TLS (transport layer security)



Шифр набор	Установка соединения, мс	Проверка сертификата, мс	Шифрование, мс	Дешифрование, мс
TLS_RSA_WITH_AES_128_CBC_SHA	101,821	0,001201	0,015668	0,035625
TLS_RSA_WITH_AES_256_CBC_SHA	107,962	0,001412	0,015681	0,041221
TLS_RSA_WITH_AES_128_CBC_SHA256	130,884	0,002176	0,015984	0,050579
TLS_RSA_WITH_AES_256_CBC_SHA256	139,963	0,004838	0,019468	0,052833

Синхронизация времени GPS/ГЛОНАСС



Высокая загруженность каналов связи потоками SV

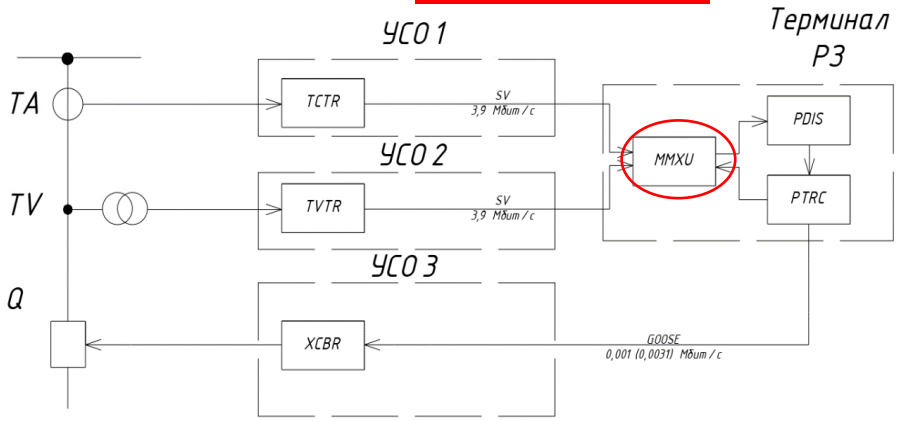
Большое количество и стоимость применяемого оборудования ЛВС

Риск потери сигналов синхронизации GPS\ГЛОНАСС

ТРЕБУЕТСЯ СОЗДАНИЕ НОВЫХ СПОСОБОВ ПЕРЕДАЧИ И СИНХРОНИЗАЦИИ ИЗМЕРЕНИЙ

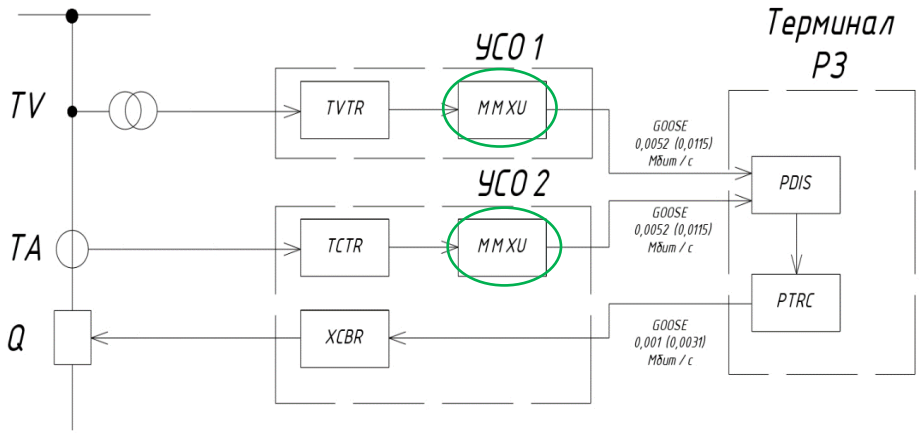
Новый способ передачи измерений в технологической сети передачи данных

15,616 Мбит/с

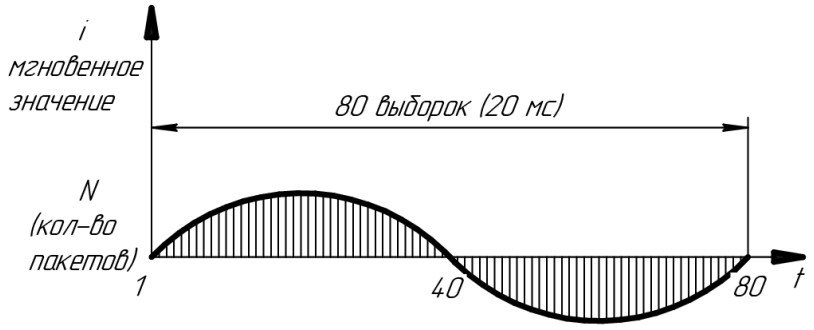


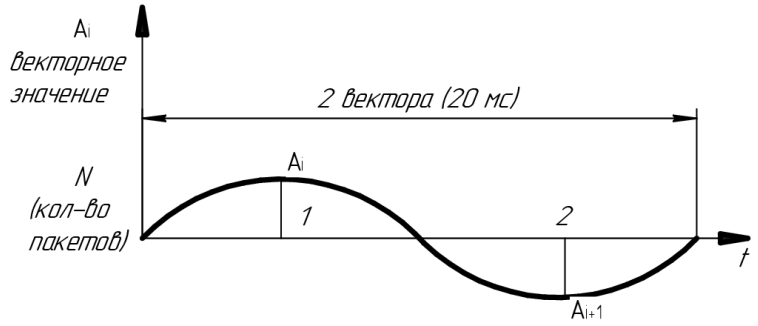
Упрощенная структура комплекса РЗА при передаче измерений по протоколу SV.

0,04588 Мбит/с



Упрощенная структура комплекса РЗА при передаче измерений с использованием GOOSE-сообщений.

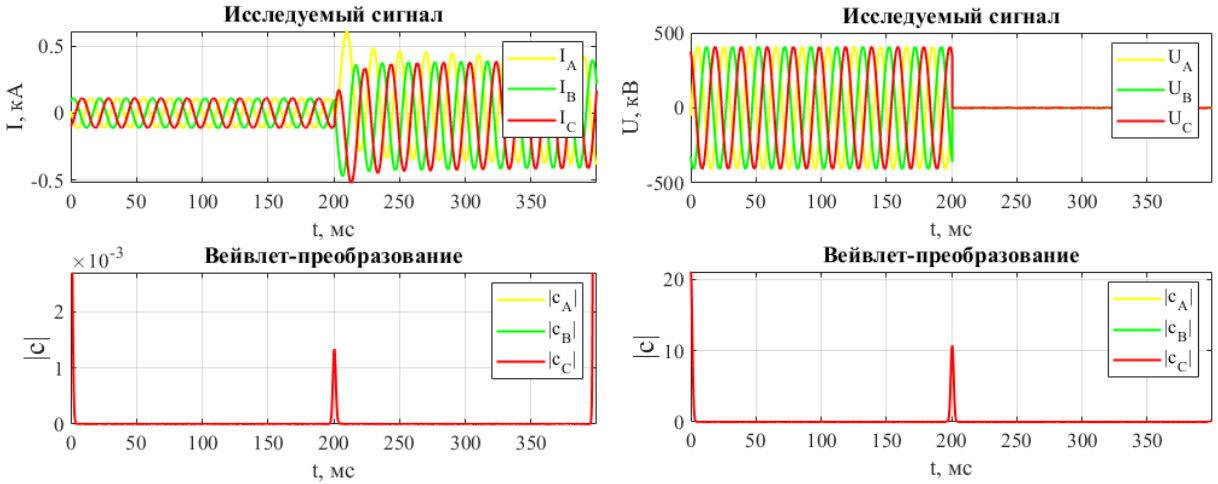




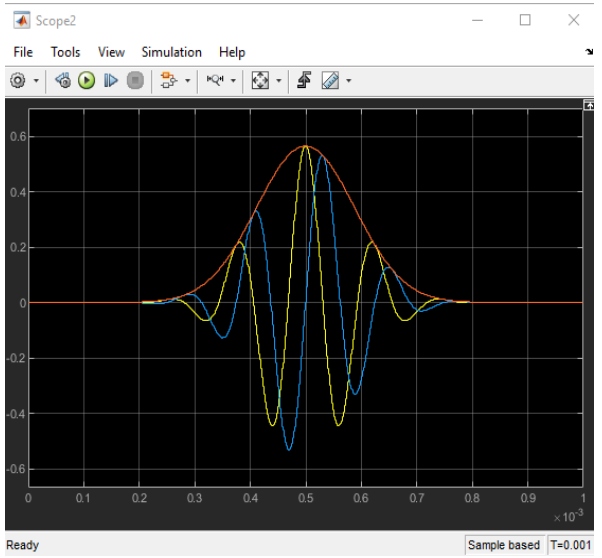
Новый способ синхронизации измерений для целей цифровой дистанционной защиты

$$CWT^{\psi}(\tau, s) = \frac{1}{\sqrt{|s|}} \int f(t) \cdot \psi_{jk}^{*}\left(\frac{t-\tau}{s}\right) dt$$

$$\psi_{jk}(t) = \frac{1}{\sqrt{\pi f_{\text{п}}}} e^{-\frac{t}{f_{\text{п}}}} e^{j2\pi f_{\text{ц}} t},$$

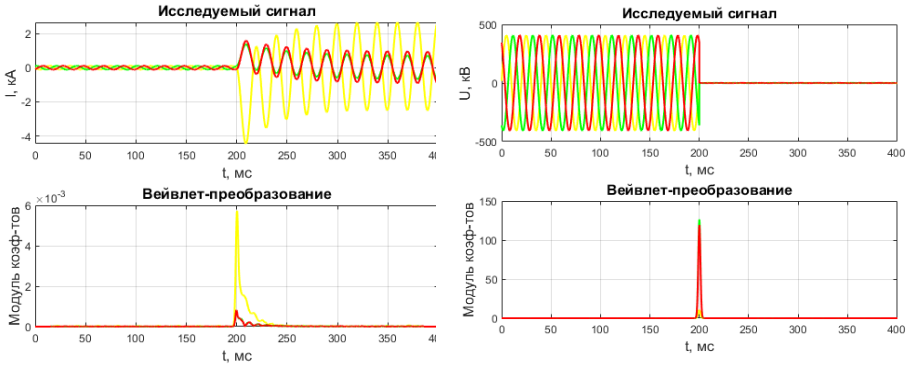


Пример определения коэффициентов вейвлет преобразования в момент возникновения короткого замыкания

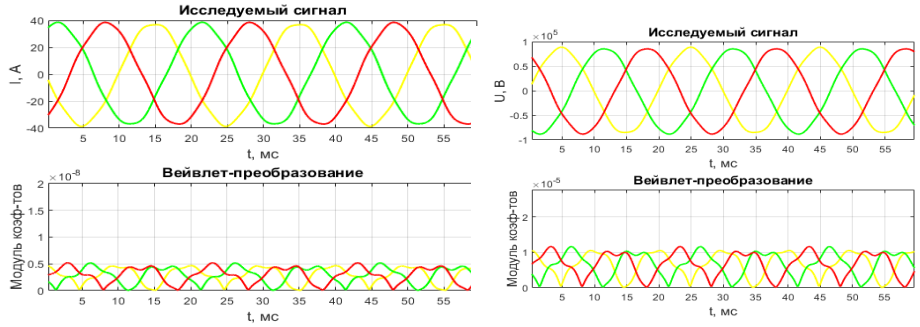


Пример материнского вейвлета Морле

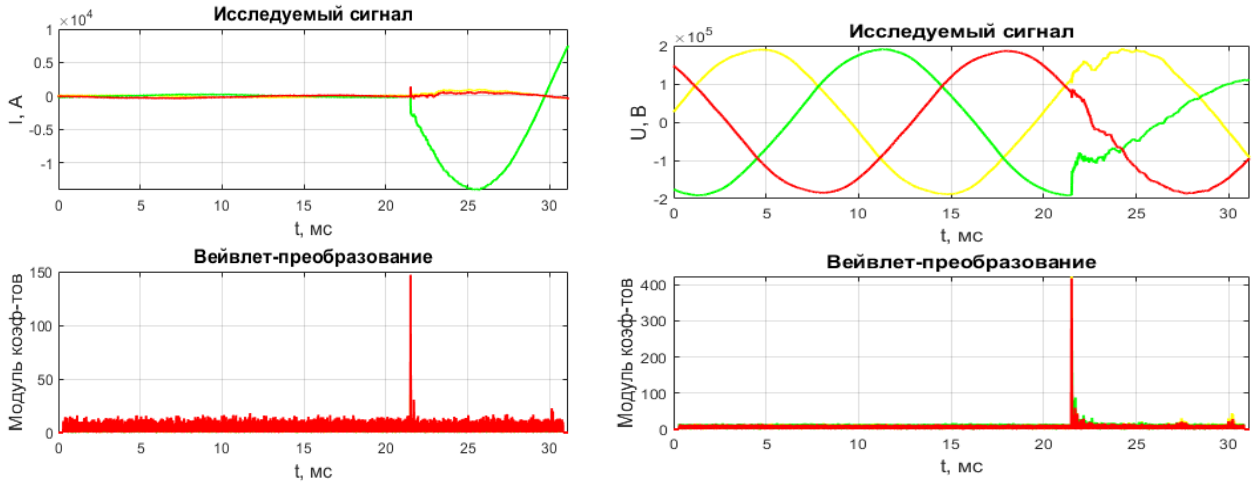
Новый способ синхронизации измерений для целей цифровой дистанционной защиты



Однофазное КЗ



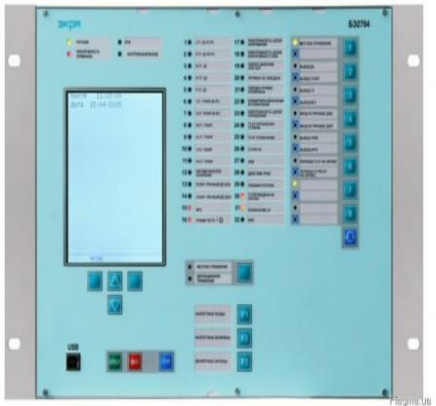
Несинусоидальный режим



Реальный случай короткого замыкания

Оценка надежности и технико-экономической эффективности разработанных решений.

Традиционный вариант передачи сигнала



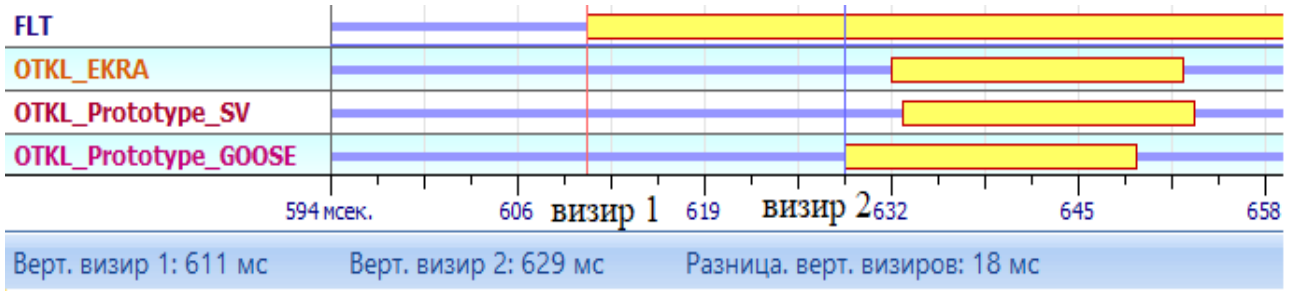
Терминал защиты ЭКРА ШЭ2607 021

SV+GOOSE

Промышленный компьютер

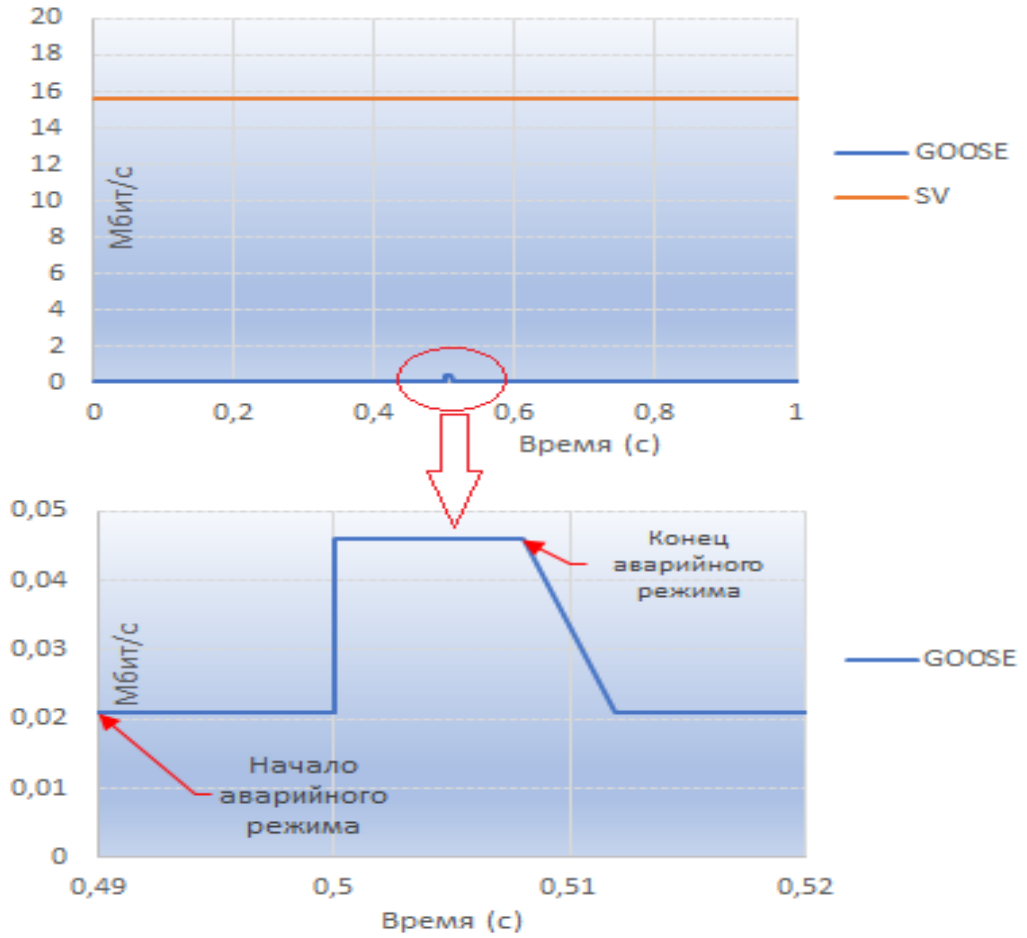
GOOSE+GOOSE

Промышленный компьютер



Сравнение времени выполнения функций РЗ

Оценка надежности и технико-экономической эффективности разработанных решений.



Загруженность канала связи ЛВС при передаче SV потока (1 режим) и GOOSE-сообщений (2 режим).

Свидетельство о регистрации патентов разрабатываемых способов и устройств

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 194579

УСТРОЙСТВО БЛОКИРОВКИ ДИСТАНЦИОННОЙ ЗАЩИТЫ В НАГРУЗОЧНЫХ РЕЖИМАХ РАБОТЫ ЭНЕРГОСИСТЕМ

Патентообладатель: *Акционерное общество "Системный оператор Единой энергетической системы" (RU)*

Авторы: *Говорун Михаил Николаевич (RU), Воробьёв Виктор Станиславович (RU), Москаленко Вадим Васильевич (RU), Расщепляев Антон Игоревич (RU), Волошин Александр Александрович (RU), Бусыгин Тимофей Григорьевич (RU), Благоразумов Дмитрий Олегович (RU)*

Заявка № 2019121495
Приоритет полезной модели 09 июля 2019 г.
Дата государственной регистрации в Государственном реестре полезных моделей Российской Федерации 17 декабря 2019 г.
Срок действия исключительного права на полезную модель истекает 09 июля 2029 г.

Руководитель Федеральной службы по интеллектуальной собственности Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2738887

Способ передачи измерений в технологической сети передачи данных

Патентообладатель: *федеральное государственное бюджетное образовательное учреждение высшего образования "Национальный исследовательский университет "МЭИ" (ФГБОУ ВО "НИУ "МЭИ") (RU)*

Авторы: *Благоразумов Дмитрий Олегович (RU), Волошин Евгений Александрович (RU), Волошин Александр Александрович (RU)*

Заявка № 2020122479
Приоритет изобретения 07 июля 2020 г.
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 18 декабря 2020 г.
Срок действия исключительного права на изобретение истекает 07 июля 2040 г.

Руководитель Федеральной службы по интеллектуальной собственности Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2740360

Способ синхронизации по времени устройств РЗА с использованием параметров аварийного режима

Патентообладатель: *федеральное государственное бюджетное образовательное учреждение высшего образования "Национальный исследовательский университет "МЭИ" (ФГБОУ ВО "НИУ "МЭИ") (RU)*

Авторы: *Благоразумов Дмитрий Олегович (RU), Волошин Евгений Александрович (RU), Волошин Александр Александрович (RU), Лебедева Наталья Сергеевна (RU)*

Заявка № 2020121127
Приоритет изобретения 25 июня 2020 г.
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 13 января 2021 г.
Срок действия исключительного права на изобретение истекает 25 июня 2040 г.

Руководитель Федеральной службы по интеллектуальной собственности Г.П. Ивлиев

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Телеграм канал Центра НТИ МЭИ

Вопросы?

Волошин Александр Александрович

Директор Центра НТИ МЭИ
К.т.н., доцент
Почетный доктор электротехники
Чл.-корр. АЭН РФ

voloshinaa@mpei.ru

http://ЦДЭС.РФ