Опыт оценки соответствия требованиям безопасности информации устройств РЗиА в ПАО «Россети» на примере терминалов серии ЭКРА 200.

Результаты и выводы НПП «ЭКРА»

ЭКРА

Текущее положение. Первое аттестованное устройство РЗА по ИБ в ПАО Россети

Согласовано
Заместитель начальника Департамента обеспечения безопасности ПАО «Россети»

Д.И. Хижкин
«____» август 2022 г.

Утверждаю
Временно исполняющий обязанности Заместителя Генерального директора по цифровой трансформации ПАО «Россети»

К.Ю. Кравченко
«____» август 2022 г.

Заключение
аттестационной комиссии

ИБ-I31-001/22 от 30.08.2022

Регистрационный № _____ от _____
Срок действия: не ограничен.

Заявитель: Общество с ограниченной ответственностью Научно-производственное предприятие «ЭКРА» (ООО НПП «ЭКРА»), ИНН 2126001172

Разработчик/производитель: Общество с ограниченной ответственностью Научно-производственное предприятие «ЭКРА» (ООО НПП «ЭКРА»), ИНН 2126001172

Оборудование: Терминалы микропроцессорные серии ЭКРА 200, серийный выпуск продукции

Комплектность: согласно формулярам ЭКРА.00019-00 30 01 и ЭКРА.656122.036-02.01 ФО/10977

Соответствует требованиям по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики, утвержденных распоряжением ПАО «Россети» от 28.02.2022 № 62р

Рекомендуется для применения в составе автоматизированных систем управления технологическими процессами энергообъектов классов напряжения от 0,4 кВ до 750 кВ, до 1-й категории значимости включительно

Заключение выдано на основании результатов испытаний: АО «НТЦ ФСК ЕЭС», ООО «СОЛАР СЕКЬЮРИТИ», ИСП РАН.

Безопасность информации обеспечивается при выполнении указаний по безопасной настройке, обновлению и эксплуатации программного обеспечения в соответствии с эксплуатационной документацией, указанной в формулярах ЭКРА.00019-00 30 01 и ЭКРА.656122.036-02.01 ФО/10977

РОССЕТИ

Публичное акционерное общество
«Российские сети»
Российская Федерация
121353, Москва, ул. Беловежская, д. 4
тел.: +7 (495) 995-53-33, факс: +7 (495) 664-81-33
e-mail: info@rosseti.ru, web: www.rosseti.ru

08.11.2022 № ГГ-4037

Генеральному директору
ООО НПП «ЭКРА»

К.Н. Дони

Благодарственное письмо

Уважаемый Константин Николаевич!

Публичное акционерное общество «Федеральная сетевая компания – Россети» (ПАО «Россети») отмечает заслуги коллектива Департамента автоматизации энергосистем ООО НПП «ЭКРА» в части повышения безопасности объектов критической информационной инфраструктуры группы компаний «Россети».

ООО НПП «ЭКРА» первая компания, которая в рамках Методики проведения проверки цифрового оборудования и систем подтвердила соответствие микропроцессорных терминалов серии ЭКРА-200 и практик безопасной разработки программного обеспечения требованиям ПАО «Россети» по безопасности информации.

Надеемся, что полученный ООО НПП «ЭКРА» опыт применения практик безопасной разработки программного обеспечения и исправления уязвимостей в дальнейшем будет распространен и на другие направления разработки в Вашей компании.

Заместитель Главного инженера Г.К. Гладковский

Шарванов Э.Р.
(800) 2001881 доб. 3072

ЭКРА

Нормативно-техническая документация ПАО «Россети»

РОССЕТИ

Публичное акционерное общество «Российские сети»

ПРИКАЗ

28.08.2020 Москва № 391

Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе

В целях обеспечения надежности и безопасности объектов электросетевого комплекса ПАО «Россети», во исполнение решения Правления ПАО «Россети» (протокол от 18.06.2020 № 1012)
ПРИКАЗЫВАЮ:

1. Утвердить Методику проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе согласно приложению 1 к настоящему приказу.
2. Рекомендовать единоличным исполнительным органам ДЗО ПАО «Россети», указанных в приложении 2 к настоящему приказу, организовать деятельность ДЗО ПАО «Россети» исходя из требований настоящего приказа.
3. Контроль за исполнением настоящего приказа возложить на Заместителя Генерального директора по безопасности Палагина В.Н.

МЕТОДИКА ПАО «РОССЕТИ»

проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе

РОССЕТИ

Публичное акционерное общество «Российские сети»

РАСПОРЯЖЕНИЕ

28.02.2022 Москва № 62р

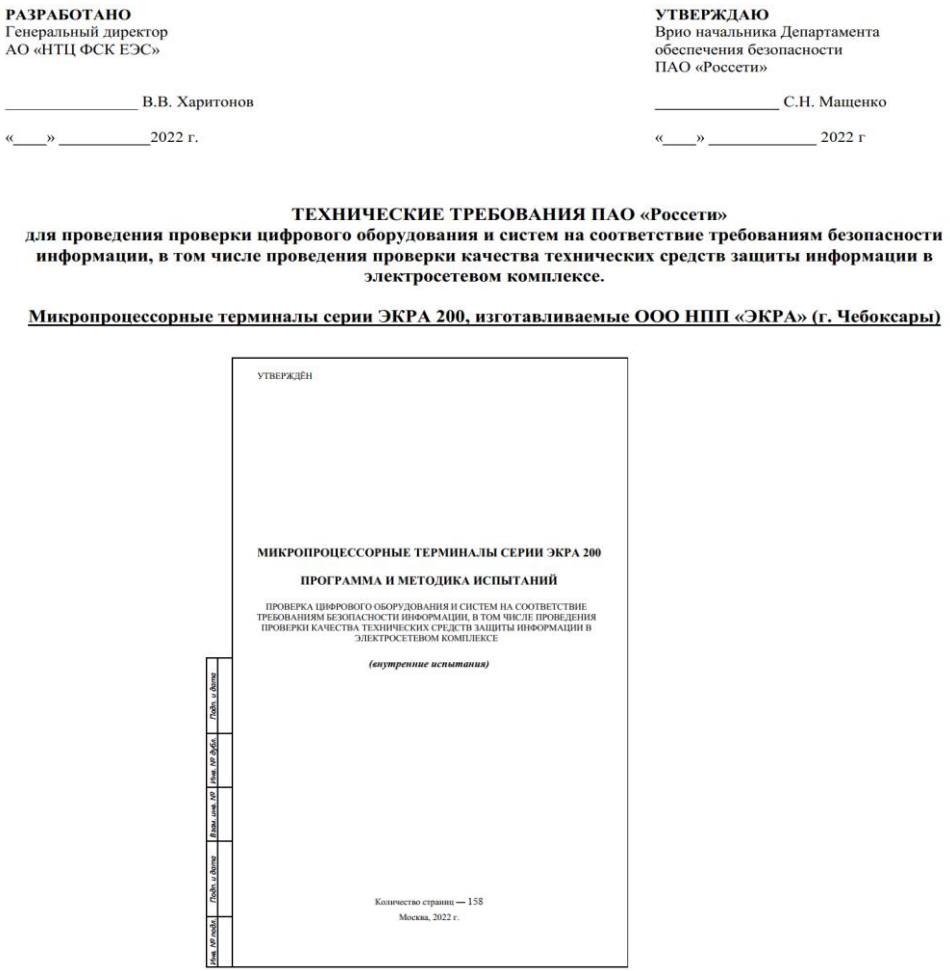
Об утверждении требований по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики

В целях проверки обеспечения требований безопасности информации микропроцессорных устройств релейной защиты и автоматики, вспомогательных систем и оборудования, от которых зависит функционирование устройств релейной защиты и автоматики, на соответствие Требованиям к оснащению линий электропередачи и оборудования объектов электроэнергетики и выше устройствами и комплексами релейной защиты и автоматики, утвержденным приказом Минэнерго России от 13.02.2019 № 101, а также к принципам функционирования устройств и комплексов релейной защиты и автоматики:

1. Утвердить Требования по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики (далее - Требования) согласно приложению, к настоящему распоряжению.
2. Временно исполняющему обязанности начальника Департамента обеспечения безопасности Мащенко С.Н. организовать оценку соответствия микропроцессорных устройств релейной защиты и автоматики, вспомогательных систем и оборудования, от которых зависит функционирование устройств релейной защиты и автоматики, Требованиям при проведении проверки качества (аттестации), регламентированной в соответствии с Методикой проведения проверки цифрового оборудования и систем, на соответствие требованиям безопасности информации в электросетевом комплексе, в том числе проверки качества технических средств защиты информации, утвержденной приказом ПАО «Россети» от 28.08.2020 № 391.
3. Контроль за исполнением настоящего распоряжения возложить на временно исполняющего обязанности начальника Департамента обеспечения безопасности Мащенко С.Н.

ЭКРА

Задачи и этапы испытаний



РАЗРАБОТАНО
Генеральный директор
АО «НТЦ ФСК ЕЭС»

_____ В.В. Харитонов

«____» _____2022 г.

УТВЕРЖДАЮ
Врио начальника Департамента
обеспечения безопасности
ПАО «Россети»

_____ С.Н. Мащенко

«____» _____ 2022 г

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ПАО «Россети»
для проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе.

Микропроцессорные терминалы серии ЭКРА 200, изготавливаемые ООО НПП «ЭКРА» (г. Чебоксары)

УТВЕРЖДЁН

МИКРОПРОЦЕССОРНЫЕ ТЕРМИНАЛЫ СЕРИИ ЭКРА 200

ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ

ПРОВЕРКА ЦИФРОВОГО ОБОРУДОВАНИЯ И СИСТЕМ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ ПРОВЕДЕНИЯ ПРОВЕРКИ КАЧЕСТВА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОСЕТЕВОМ КОМПЛЕКСЕ

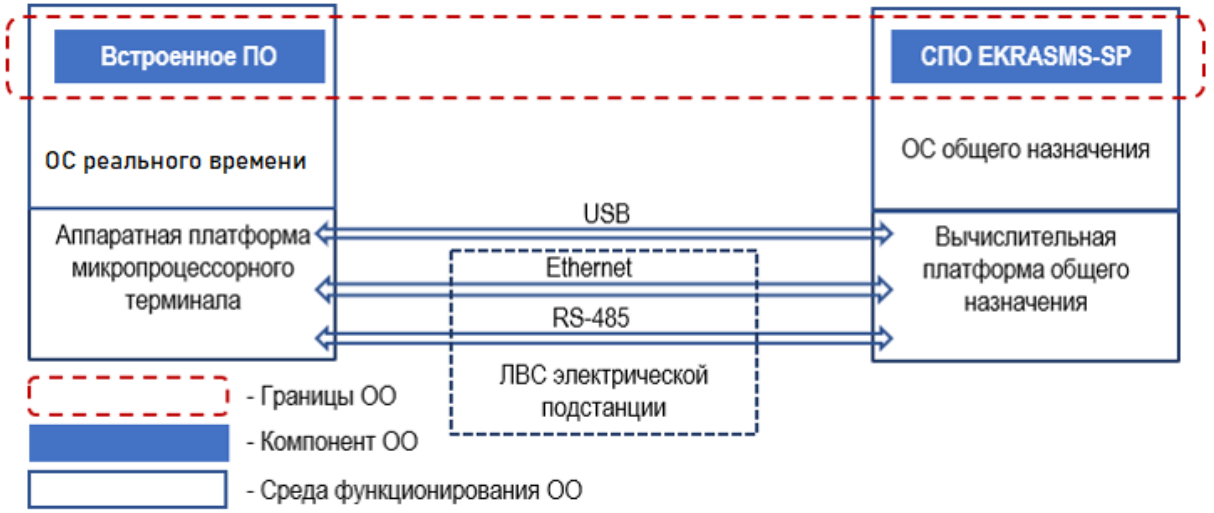
(внутренние испытания)

Количество страниц — 158

Москва, 2022 г.

- **Разработка и согласование технических требований (ТТ) по ИБ:**
  - доработка функционала безопасности информации внутреннего и прикладного ПО терминала;
  - доработка и проверка комплекта документации на ПО;
  - устранение уязвимостей внутреннего и прикладного ПО терминала (bdu.fstec.ru);
- **Предварительные испытания.**
  - подготовка программы и методики испытаний;
  - проведение предварительных испытаний;
  - оформление промежуточных протоколов и устранение замечаний;
  - проведение исследований ПО на уязвимости и недекларированные возможности при сотрудничестве с Ростелеком-Солар и ИСП РАН;
- **Проведение испытаний.**
  - Проверка реализованного функционала безопасности информации на стенде;
  - проверка комплекта документации на соответствие требованиям;
  - очная проверка состояния производства по итогам испытаний;
  - устранение замечаний по доработке документации и функционала;
  - подготовка отчетов по исследованиям на уязвимости и недекларированные возможности при сотрудничестве с Ростелеком-Солар и ИСП РАН;
  - получение заключения аттестационной комиссии;

Объект оценки



Два раздела объекта оценки:

1) встроенное в микропроцессорный терминал ЭКРА 200 программное обеспечение E3_SW91;

2) внешнее специальное программное обеспечение - программный комплекс EKRASMS-SP.

Объект оценки в Реестре российского ПО

EKRASMS-SP

Правообладатели программного обеспечения

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ "ЭКРА"
коммерческая организация без преобладающего иностранного участия

Сокращенное наименование:

ООО НПП "ЭКРА"

Государство регистрации в качестве юридического лица:

Россия

Основной государственный регистрационный номер регистрации в качестве юридического лица (ОГРН):

1022101135726

Идентификационный номер (ИНН):

2126001172

Сведения об основаниях возникновения у правообладателя (правообладателей) исключительного права на программное обеспечение на территории всего мира и на весь срок действия исключительного права

Собственная разработка - Свидетельство № 2007610931 об официальной регистрации программы для ЭВМ от 28.02.2007

Запись в реестре №6731 от 09.06.2020 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 09.06.2020 №272

Класс программного обеспечения по классификатору программного обеспечения, утвержденному приказом от 31.12.2015 № 621

Основной класс:

02.11 Системы мониторинга и управления

Описание программного обеспечения

Коды продукции в соответствии с Общероссийским классификатором продукции по видам экономической деятельности:

58.29.29 Обеспечение программное прикладное прочее на электронном носителе

58.29.32 Обеспечение программное прикладное для загрузки

Наличие функционала поддержки работы пользователей с ограничениями по слуху:

Нет

Наличие функционала поддержки работы пользователей с ограничениями по зрению:

Нет

Адрес страницы сайта правообладателя, на которой размещена документация, содержащая описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения:

Программа E3_SW91 для терминалов серии ЭКРА 200

Правообладатели программного обеспечения

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ "ЭКРА"
коммерческая организация без преобладающего иностранного участия

Сокращенное наименование:

ООО НПП "ЭКРА"

Государство регистрации в качестве юридического лица:

Россия

Основной государственный регистрационный номер регистрации в качестве юридического лица (ОГРН):

1022101135726

Идентификационный номер (ИНН):

2126001172

Сведения об основаниях возникновения у правообладателя (правообладателей) исключительного права на программное обеспечение на территории всего мира и на весь срок действия исключительного права

ЭКРА.00023 - 01 90 01 от 16.11.2012 Техническое задание

Запись в реестре №7714 от 14.12.2020 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 07.12.2020 №706

Класс программного обеспечения по классификатору программного обеспечения, утвержденному приказом от 31.12.2015 № 621

Основной класс:

02.11 Системы мониторинга и управления

Описание программного обеспечения

Коды продукции в соответствии с Общероссийским классификатором продукции по видам экономической деятельности:

58.29.12 Обеспечение программное сетевое на электронном носителе

Наличие функционала поддержки работы пользователей с ограничениями по слуху:

Нет

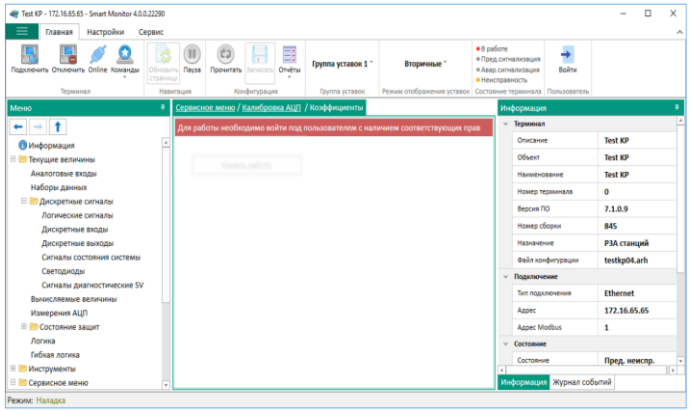
Наличие функционала поддержки работы пользователей с ограничениями по зрению:

Нет

Адрес страницы сайта правообладателя, на которой размещена документация, содержащая описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения:

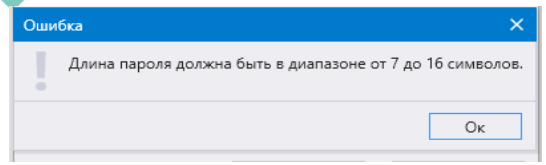
https://soft.ekra.ru/smssp/ru/main/

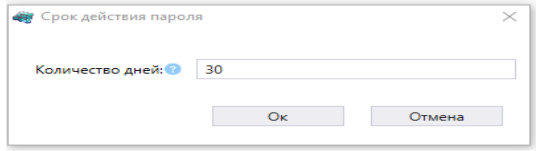
Релизация технических требований в встроенном и прикладном ПО терминала

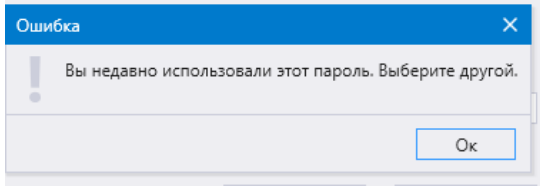


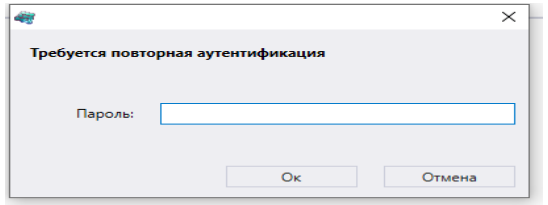
- Идентификация и аутентификация пользователей;
- Защита аутентификационной информации при передаче;
- Регистрация событий безопасности;
- Защита информации о событиях безопасности;
- Разделение полномочий (ролей) пользователей;
- Доверенная загрузка;
- Ограничение неуспешных попыток доступа;
- Блокирование сеанса доступа пользователя при неактивности;
- Ограничение числа параллельных сеансов доступа;
- Контроль использования СМНИ (съемных машинных носителей информации);
- Обеспечение целостности и доступности;
- Восстановление информации при нештатных ситуациях;
- Идентификация объектов управления конфигурацией;
- Контроль действий по внесению изменений;
- Управление обновлениями ПО.

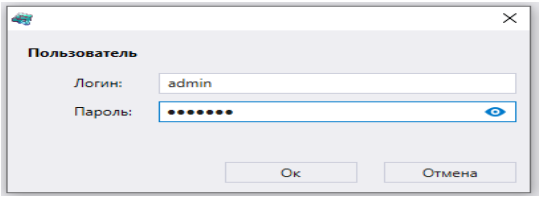
Идентификация и аутентификация пользователей





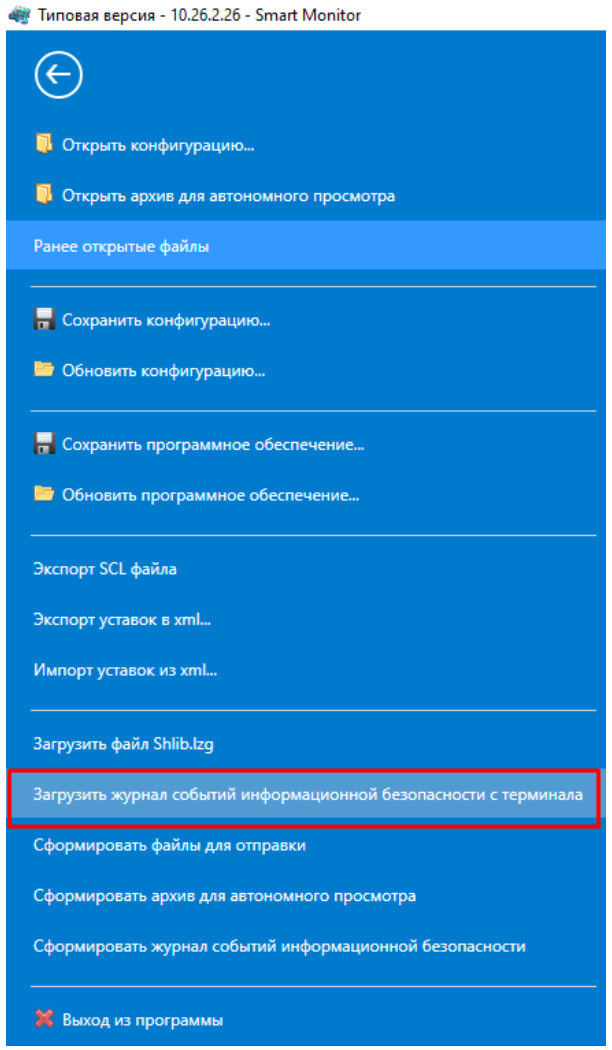






- Запрет установки пароля менее семи цифровых символов.
- Единые учетные записи в терминале и прикладном ПО.
- Установка срока действия (времени жизни) пароля.
- Запрет использования старых паролей (не менее 4 паролей).
- Аутентификационная информация (пароль) не передается по сети в открытом виде по модифицированному для безопасной авторизации пользователей протоколу Modbus.
- Аутентификационная информация (пароль) хранится в терминале в нечитаемом виде, (не позволяющем восстановить пароль).
- Авторизованный доступ к терминалу завершается по тайм-ауту (при бездействии), либо самим пользователем.
- Маскирование пароля при вводе пользователем.

Журнал событий безопасности



- Отдельный встроенный журнал событий ИБ в терминале.
- Хранение журнала событий ИБ во внутренней энергонезависимой памяти терминала.
- Глубина хранения событий ИБ – не менее 8000 записей.
- Запись событий ИБ выполняется постоянно (после включения терминала).
- Записи журнала событий ИБ содержат необходимые атрибуты: идентификатор (пользователь либо процесса), дата/время, тип, источник, протокол и порт подключения, результат (успешный/неуспешный).
- События ИБ имеют уникальный номер, присвоение номеров происходит по сквозному принципу.
- При сбросе терминала к заводским настройкам, записи журналов ИБ сохраняются.
- Предусмотрена функция циклической перезаписи самых старых записей, новыми записями с соответствующим сбросом сквозной нумерации событий.
- Записи журнала событий ИБ сортируются по номерам и датам создания.
- В журнале ИБ фиксируются события в соответствии с перечнем из ТТ.
- Запрещено удаление/изменение записей в журнале событий ИБ.
- Разграничен доступ к скачиванию и чтению журналов событий ИБ в соответствии с ролевой моделью.

Перечень событий в журнале ИБ

№ п/п	Наименование событий безопасности
1	Загрузка (останов), перезагрузка устройства
2	Проверка контрольных сумм файлов программного обеспечения и конфигурации
3	Подключение к сервисному порту
5	Запрос на параллельный сеанс доступа к устройству
6	Использование механизма аутентификации
7	Превышение количества неудачных попыток аутентификации
8	Переход устройства в сервисный режим
9	Сброс программного обеспечения до заводских настроек
10	Обновление системного или прикладного программного обеспечения
11	Изменение конфигурации устройства: логики работы, настроек, уставок
12	Включение и выключение портов связи
13	Изменения настроек синхронизации времени, текущей даты/времени
14	Создание, редактирование, удаление ролей пользователей, изменение паролей пользователей
15	Использование съемных носителей информации

```
| 3959 |  [08/06/2022 11:07:56]  FIA_UAU.2 |          lcd  |       engineer  | 1 |  Пользователь аутентифицирован через дисплей устройства
| 3960 |  [08/06/2022 11:08:34]  FDP_ROL.2 |      service  |       engineer  | 1 |  Запрос на восстановление заводских ПО и конфигурации.
| 3961 |  [08/06/2022 11:09:11]  FMT_MTD.1 |          lcd  |       engineer  | 1 |  Применения файлов ПО и конфигурации выполнено успешно
| 3962 |  [08/06/2022 11:10:04]  FMT_MTD.1 |         main  |       engineer  | 1 |  Обновление конфигурации и программы завершено успешно.
| 3963 |  [08/06/2022 11:10:23]  FDP_ACF.1 |         main  |                 | 1 |  Дата и время предыдущего выкл. терминала 08/06/2022 11:04:01

| 3964 |  [08/06/2022 11:10:23]  FMT_SMF.1 |         main  |                 | 1 |  Время включения терминала: 08/06/2022 11:10:23
| 3965 |  [08/06/2022 11:10:23]  FMT_SMF.1 |         main  |                 | 1 |  Запуск логирования событий информационной безопасности
| 3966 |  [08/06/2022 11:10:40]  FDP_SDI.2 |     archiver  |                 | 1 |  Проверка контроля целостности файла прошивки прошла успешно.
| 3967 |  [08/06/2022 11:10:40]  FDP_SDI.2 |     archiver  |                 | 1 |  Проверка контроля целостности файла конфигурации прошла успешно.
| 3968 |  [08/06/2022 11:10:40]  FDP_SDI.2 |     archiver  |                 | 1 |  Проверка контроля целостности архива прав доступа прошла успешно.
```

Разделение полномочий по ролям пользователей

Администрирование пользователей

Пользователи | Группы | Права

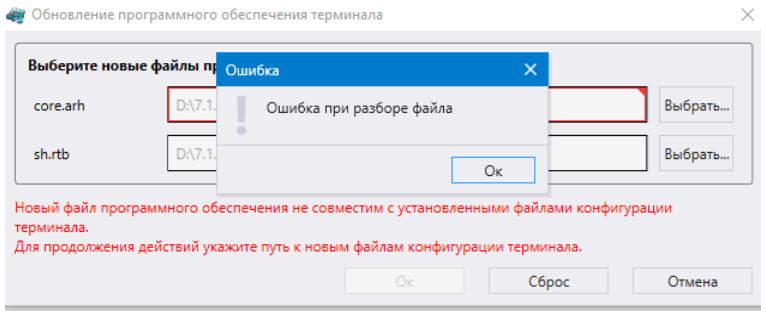
	g_administrator	g_serviceman_acs
Параметры аналоговых входов		+
Параметры ввода/вывода дискретных входов(жёсткая логика)		+
Параметры защит		+
Параметры матрицы(жёсткая логика)		+
Параметры матрицы(гибкая логика)		+
Параметры логических элементов (жёсткая логика)		+
Параметры логических элементов (гибкая логика)		+
Параметры осциллографирования сигналов		+
Параметры регистрирования сигналов		+
Параметры расчёта ресурса КА		+
Запись уставок и обновление ПО,конфигурации		+
Параметры связи		+
Параметры коэффициентов сглаживания вычисляемых величин		+
Калибровка аналоговых блоков		+
Параметры дискретных блоков		+
Параметры синхронизации		+
Параметры языка меню		+
Изменение системного времени		+
Тест индикации		+
Тест выходных реле		+
Тест goose		+
T_SV		+
Автоматическое тестирование		+
Мнемосхема, управление		+
Запись по FTP		
Яркость светодиодов		+
Яркость подсветки		+
Меню Usb привода		+
Управление по 61850		+
Уставки вычисляемых величин		+
Параметры приемника		+
Параметры передатчика		+
Управление,ЭКУ,мнемосхема		+
Доступ к чтению журнала событий ИБ	+	+
Администрирование пользователей	+	
Настройка параметров дисплея		+
Сброс на заводские настройки		+
Перевод терминала в сервисный режим		+
Сброс сигнализации по протоколу modbus		+

Права доступа настраиваются ролям пользователей «Администратор» и «Инженер» в соответствии с требованиями:

👉пользователю с ролью «Администратор» настраиваются права для создания/ редактирования/ удаления ролей и учетных записей пользователей, изменения паролей, чтения событий в журнале событий безопасности с запретом возможности обновления системного ПО и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства.

👉 пользователю с ролью «Инженер» настраиваются права для обновления системного программного обеспечения и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства, чтения журнала событий безопасности с запретом возможности назначения и(или) изменения паролей сторонних учетных записей.

Доверенная загрузка



Сервисное меню / Диагностика блоков

Наименование	Тип блока	Состояние
E6	П2632	Исправен
E1	Л2632	Предупр. или авар. неисправность блока
E8	В1291	Исправен
E2	Р1721	Исправен
E5	Д2798	Исправен
E4	Э2693	Исправен
E3	К1182	Исправен

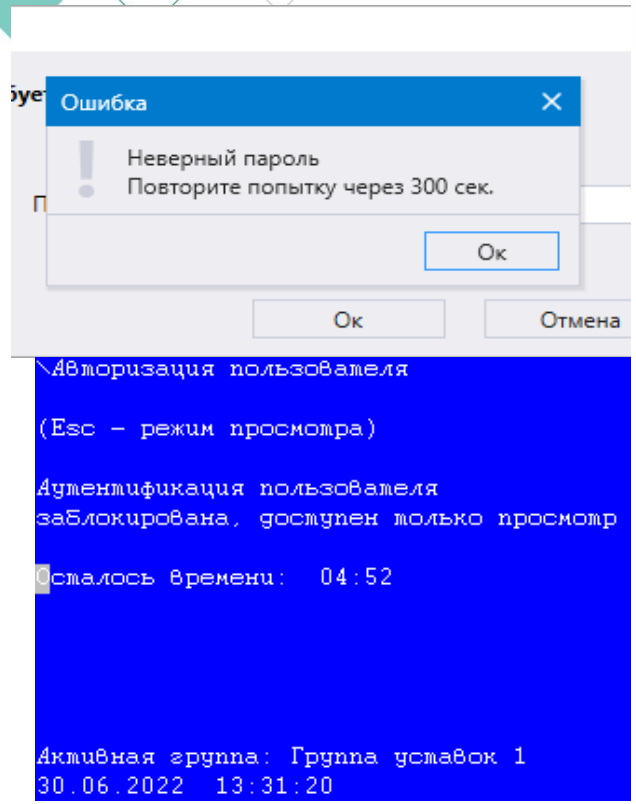
Доверенная загрузка обеспечивает исключение несанкционированного доступа к программным и/или техническим ресурсам терминала на этапе его загрузки, посредством:

👉 блокирования попыток несанкционированной загрузки нештатной операционной системы/встроенного ПО;

👉 контроля целостности ПО, компонентов ПО и аппаратных компонентов (блоков) терминала

```
| 3964 |  [08/06/2022 11:10:23]  FMT_SMF.1 |          main |  | 1 |  Время включения терминала: 08/06/2022 11:10:23
| 3965 |  [08/06/2022 11:10:23]  FMT_SMF.1 |          main |  | 1 |  Запуск логирования событий информационной безопасности
| 3966 |  [08/06/2022 11:10:40]  FDP_SDI.2 |      archiver |  | 1 |  Проверка контроля целостности файла прошивки прошла успешно.
| 3967 |  [08/06/2022 11:10:40]  FDP_SDI.2 |      archiver |  | 1 |  Проверка контроля целостности файла конфигурации прошла успешно.
| 3968 |  [08/06/2022 11:10:40]  FDP_SDI.2 |      archiver |  | 1 |  Проверка контроля целостности архива прав доступа прошла успешно.
```

Ограничение неуспешных попыток доступа



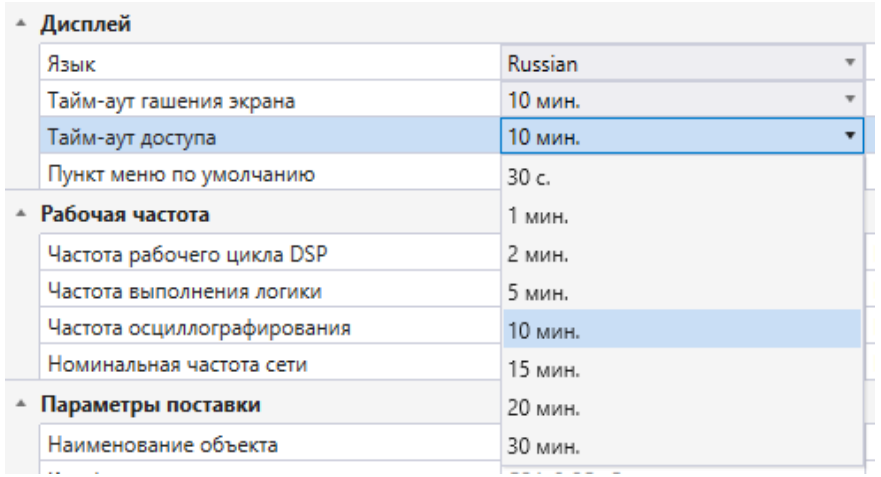
👉 функции безопасности терминала ограничивают количество неуспешных попыток аутентификации (до блокирования учетной записи – 3 попытки);

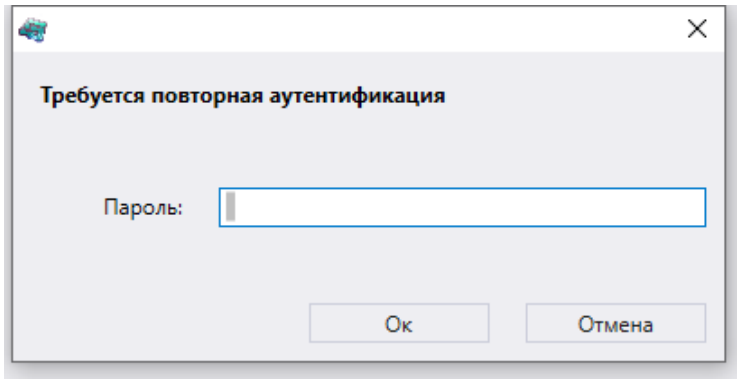
👉 при превышении заданного количества неуспешных попыток аутентификации функции безопасности терминала выполняют блокировку доступа к терминалу на заданный период времени, при этом фиксируется событие в журнале событий ИБ;

👉 после успешной аутентификации пользователя, счетчик неуспешных попыток аутентификации обнуляется;

4328	[08/06/2022 15:45:16]	FIA_UAU.2	lcd		1	Введен неверный пароль 1 раз
4329	[08/06/2022 15:45:20]	FIA_UAU.2	lcd		1	Введен неверный пароль 2 раз
4330	[08/06/2022 15:45:23]	FIA_UAU.2	lcd		1	Введен неверный пароль 3 раз
4331	[08/06/2022 15:45:23]	FIA_UAU.2	lcd		1	Блокировка ИЧМ - превышено количество неверного ввода пароля
4332	[08/06/2022 15:46:11]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 1 раз.
4333	[08/06/2022 15:46:13]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 2 раз.
4334	[08/06/2022 15:46:14]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 3 раз.
4335	[08/06/2022 15:46:14]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Блокировка ИЧМ - превышено количество неверного ввода пароля.
4336	[08/06/2022 15:50:23]	FTA_SSL.1	lcd		1	Разблокировка ИЧМ

Блокирование сеанса доступа пользователя при неактивности

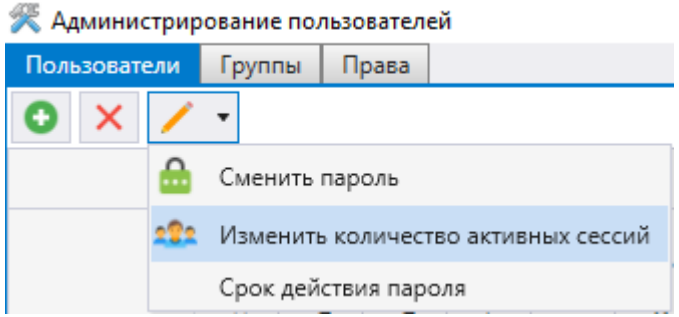


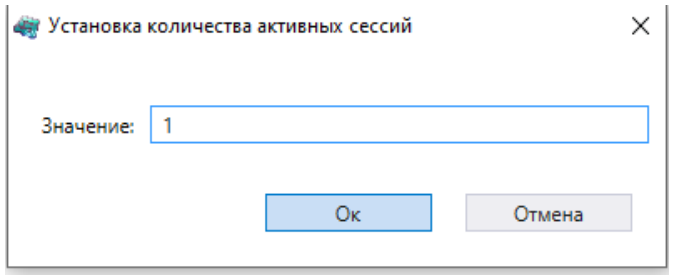


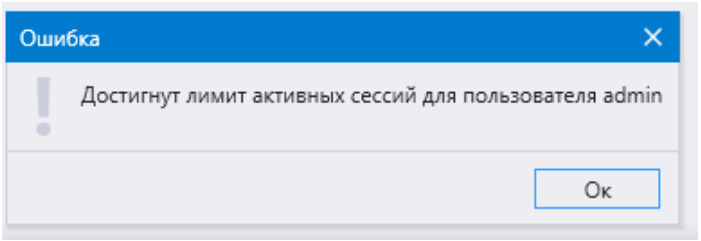
👉 функции безопасности блокируют сеанс авторизованного пользователя по истечении, заданного интервала времени бездействия авторизованного пользователя;

👉 функции безопасности обеспечивают настройку интервала времени бездействия авторизованного пользователя, по истечении которого блокируется сеанс;

Ограничение числа параллельных сеансов доступа







- Функционал терминала не допускает наличие параллельных сеансов пользователей.
- Попытки запроса на параллельный (одновременный) сеанс фиксируются в журнале событий безопасности.

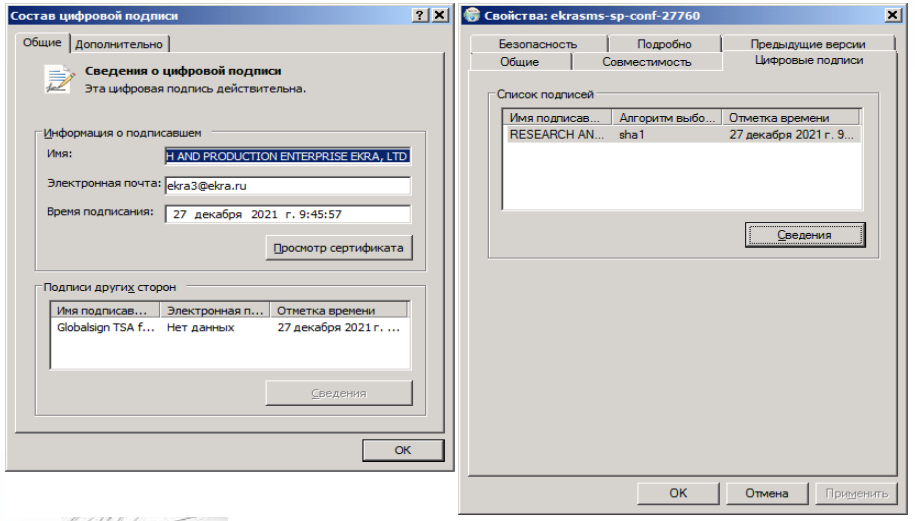
4599	[09/06/2022 11:05:53]	FIA_UAU.2	modbus	Инженер	1	Пользователь подключился
4600	[09/06/2022 11:06:51]	FIA_UAU.2	modbus	Инженер	1	Попытка превышения количества активных сессий пользователя. Параллельные сеансы запрещены
4601	[09/06/2022 11:06:57]	FIA_UAU.2	modbus	Инженер	1	Пользователь отключился от modbus сервера

Контроль использования съемных носителей информации

- В терминале обеспечивается контроль использования съемных носителей информации на интерфейсах терминала, путем фиксации фактов подключения в журнале событий безопасности.
- Обновление ПО и конфигурации терминала с съемных носителей информации возможно только после авторизации пользователя с соответствующими правами.

4626	[09/06/2022 11:45:14]	FMT_MTD.1	lcd		1	Подключен внешний USB диск d:\ Id: 4096 (Mass Storage Device), Vendor: 34148 (JetFlash), Serial#: 9G8X0BX0
4627	[09/06/2022 11:45:28]	FIA_UAU.2	lcd	Инженер	1	Пользователь аутентифицирован через дисплей устройства
4628	[09/06/2022 11:46:04]	FIA_UAU.2	modbus	Инженер	1	Пользователь отключился по таймауту
4629	[09/06/2022 11:46:04]	FIA_UAU.2	modbus	Инженер	1	Пользователь подключился
4630	[09/06/2022 11:47:07]	FMT_MTD.1	lcd	Инженер	1	Отключен внешний USB диск d:\

Обеспечение целостности

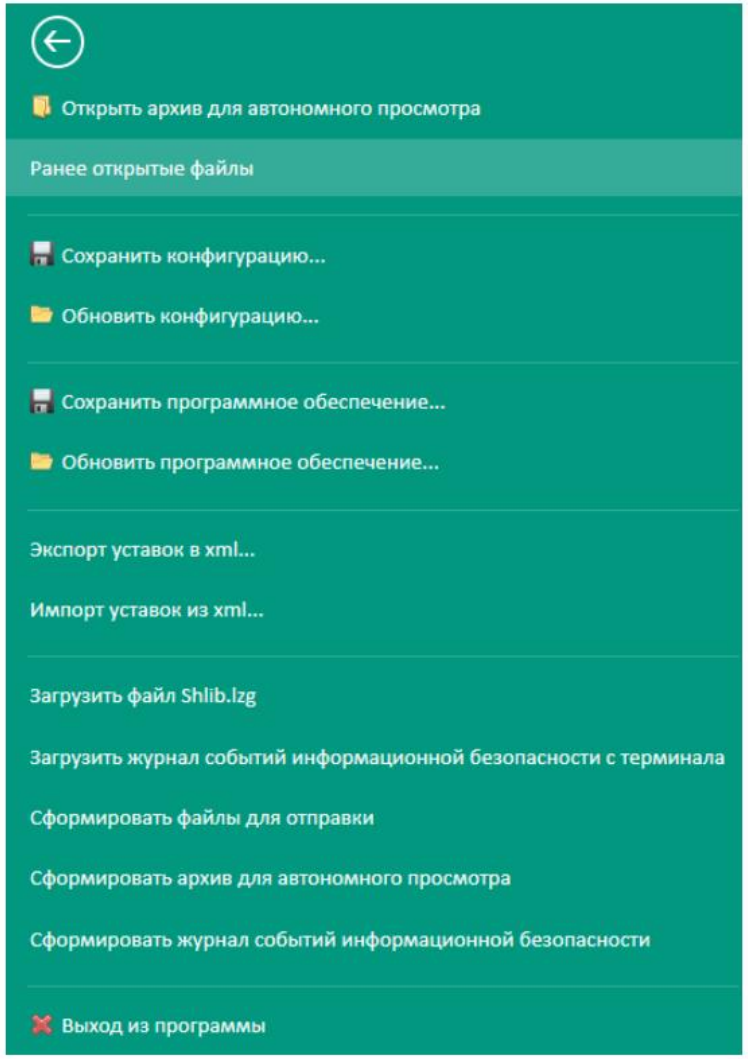


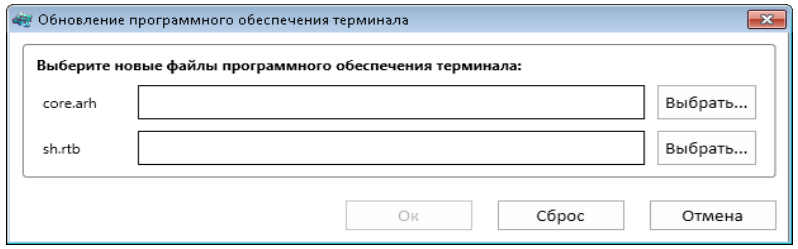
- Система самодиагностики терминала непрерывно выполняет проверку целостности исполняемой программы и данных (стартовая и циклическая, не реже 1 раза в сутки). В журнале ИБ фиксируются события проверки целостности ПО терминала, при загрузке и в процессе работы терминала.
- Терминал блокирует выходные воздействия и формирует соответствующую сигнализацию при обнаружении системой самодиагностики нарушения целостности исполняемой программы или данных.
- Результаты отрицательных проверок целостности исполняемой программы или данных фиксируются в журнале событий безопасности.

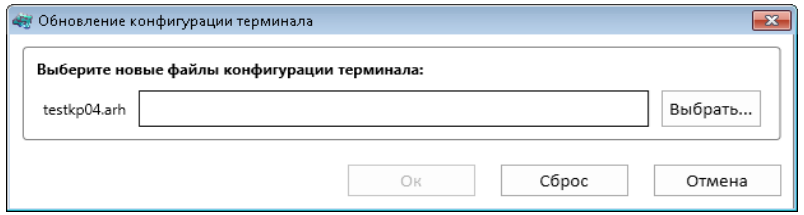
3964	[08/06/2022 11:10:23]	FMT_SMF.1	main		1	Время включения терминала: 08/06/2022 11:10:23
3965	[08/06/2022 11:10:23]	FMT_SMF.1	main		1	Запуск логирования событий информационной безопасности
3966	[08/06/2022 11:10:40]	FDP_SDI.2	archiver		1	Проверка контроля целостности файла прошивки прошла успешно.
3967	[08/06/2022 11:10:40]	FDP_SDI.2	archiver		1	Проверка контроля целостности файла конфигурации прошла успешно.
3968	[08/06/2022 11:10:40]	FDP_SDI.2	archiver		1	Проверка контроля целостности архива прав доступа прошла успешно.

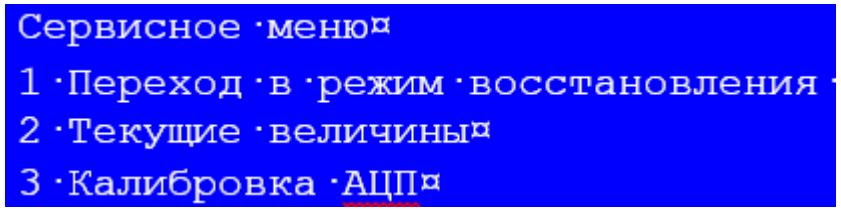
4503	[08/06/2022 23:47:56]	FDP_SDI.2	archiver		1	Периодическая проверка контроля целостности файла прошивки прошла успешно.
4504	[08/06/2022 23:47:56]	FDP_SDI.2	archiver		1	Периодическая проверка контроля целостност файла конфигурации прошла успешно.
4505	[09/06/2022 05:47:54]	FDP_SDI.2	archiver		1	Периодическая проверка контроля целостност файла прошивки прошла успешно.
4506	[09/06/2022 05:47:54]	FDP_SDI.2	archiver		1	Периодическая проверка файла конфигурации прошла успешно.

Обеспечение возможности восстановления информации при нештатных ситуациях





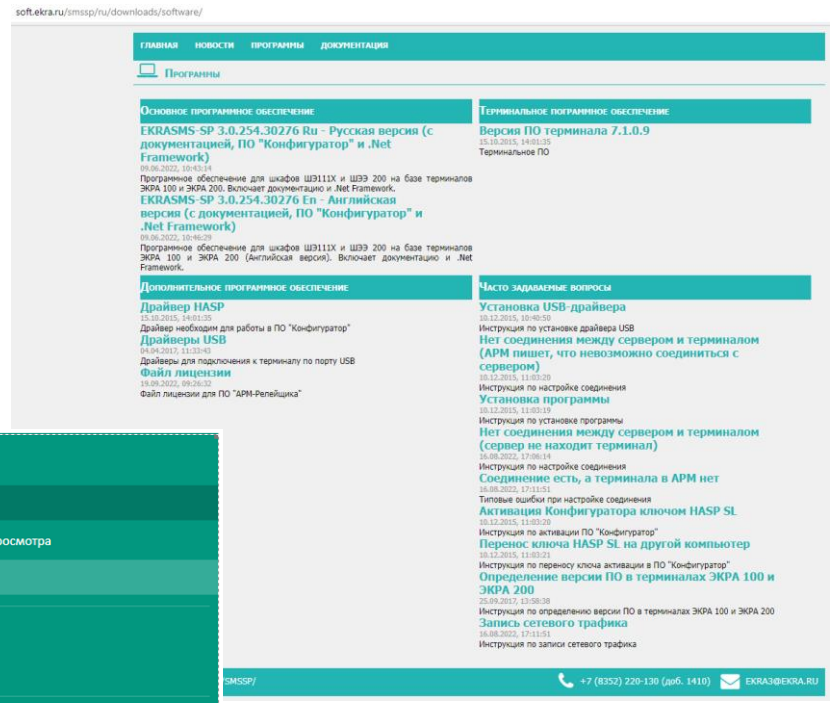


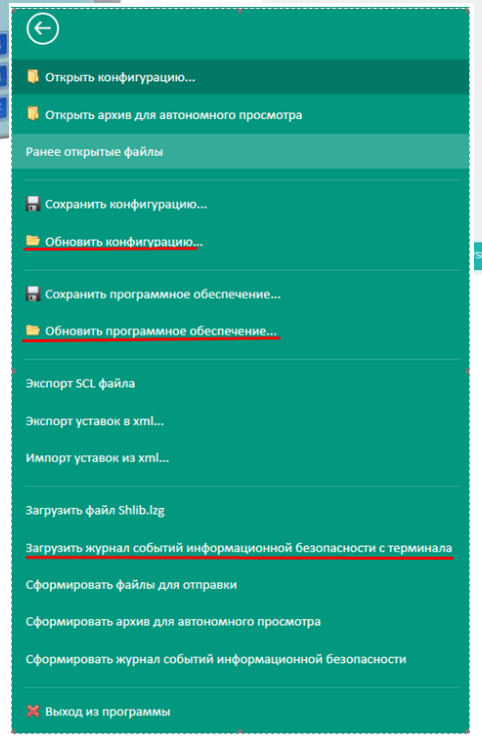


👉В терминале реализована возможность восстановления базового ПО, конфигураций, уставок с резервных копий.

👉Функции безопасности терминала обеспечивают восстановление конфигурации и ПО путем загрузки резервных копий конфигурации и ПО, посредством подключенного к терминалу переносного ПК со специализированным ПО через **сервисный порт**.

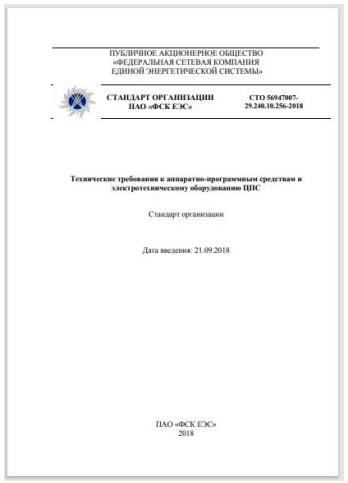
Управление конфигурацией и обновлениями ПО

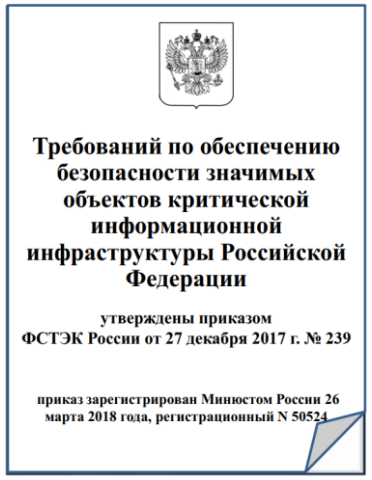


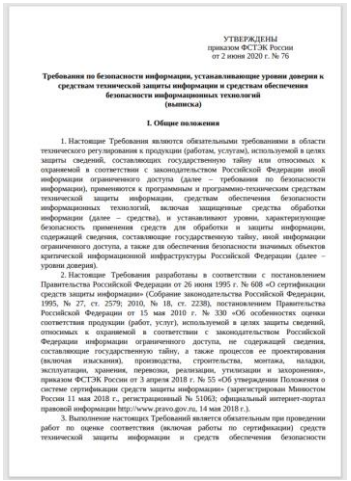


- Конфигурирование встроенного ПО терминала осуществляется после успешного прохождения процедуры аутентификации.
- Действия по внесению изменений в базовую конфигурацию терминала и его подсистемы защиты информации регистрируются с журнале событий ИБ.
- В терминале выделен сервисный интерфейс для обновления встроенного ПО.
- Обновление встроенного ПО терминала по сервисному интерфейсу выполняется посредством специального ПО, входящего в комплект поставки.
- Переключение сервисного интерфейса в режим готовности к выполнению команд по обновлению ПО осуществляется локально посредством ИЧМ.
- После обновления ПО терминала сохраняются роли и пароли пользователей, журнал событий ИБ.
- Пакеты обновлений ПО терминала с информацией о версиях пакетов обновлений, размещаются на территории РФ.

Организационно-технические требования







👉 ГОСТ Р 56939-2016. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

👉 Приказ Минэнерго России от 13.02.2019 № 101 «Об утверждении требований к оснащению линий электропередачи и оборудования объектов электроэнергетики классом напряжения 110 кВ и выше устройствами и комплексами релейной защиты и автоматики, а также к принципам функционирования устройств и комплексов релейной защиты и автоматики».

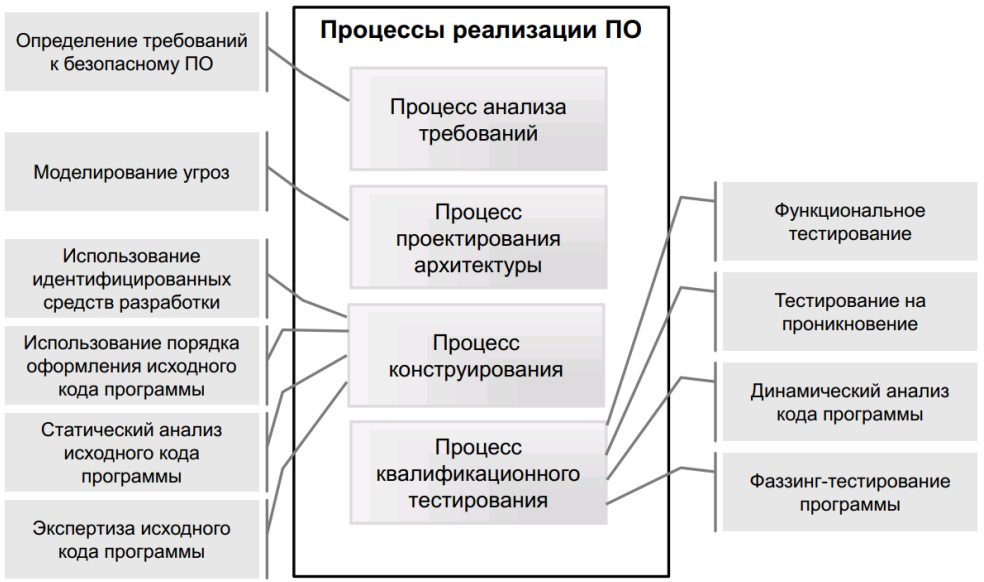
👉 Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

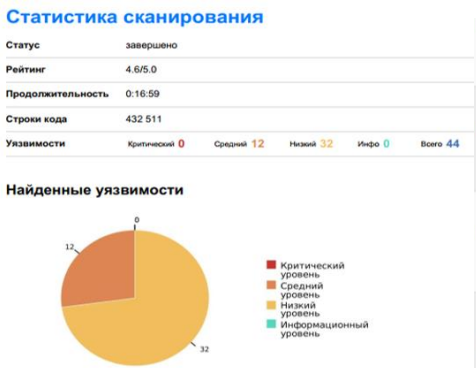
👉 Приказ ФСТЭК России от 02.06.2020 № 76 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

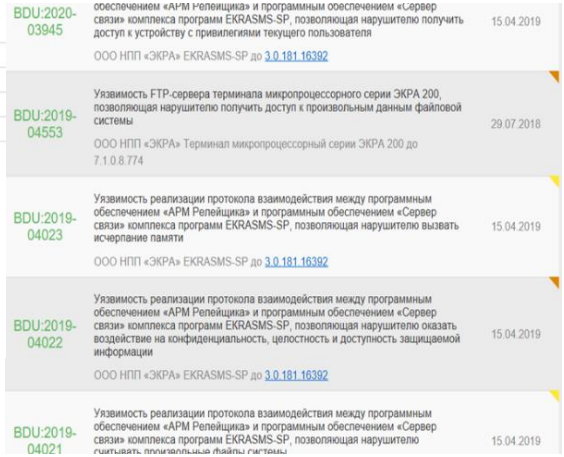
👉 СТО 56947007-29.240.10.256-2018 «Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС» (утвержден приказом ПАО «Россети» от 21.09.2018 № 355).

ЭКРА

Реализация организационно-технических требований

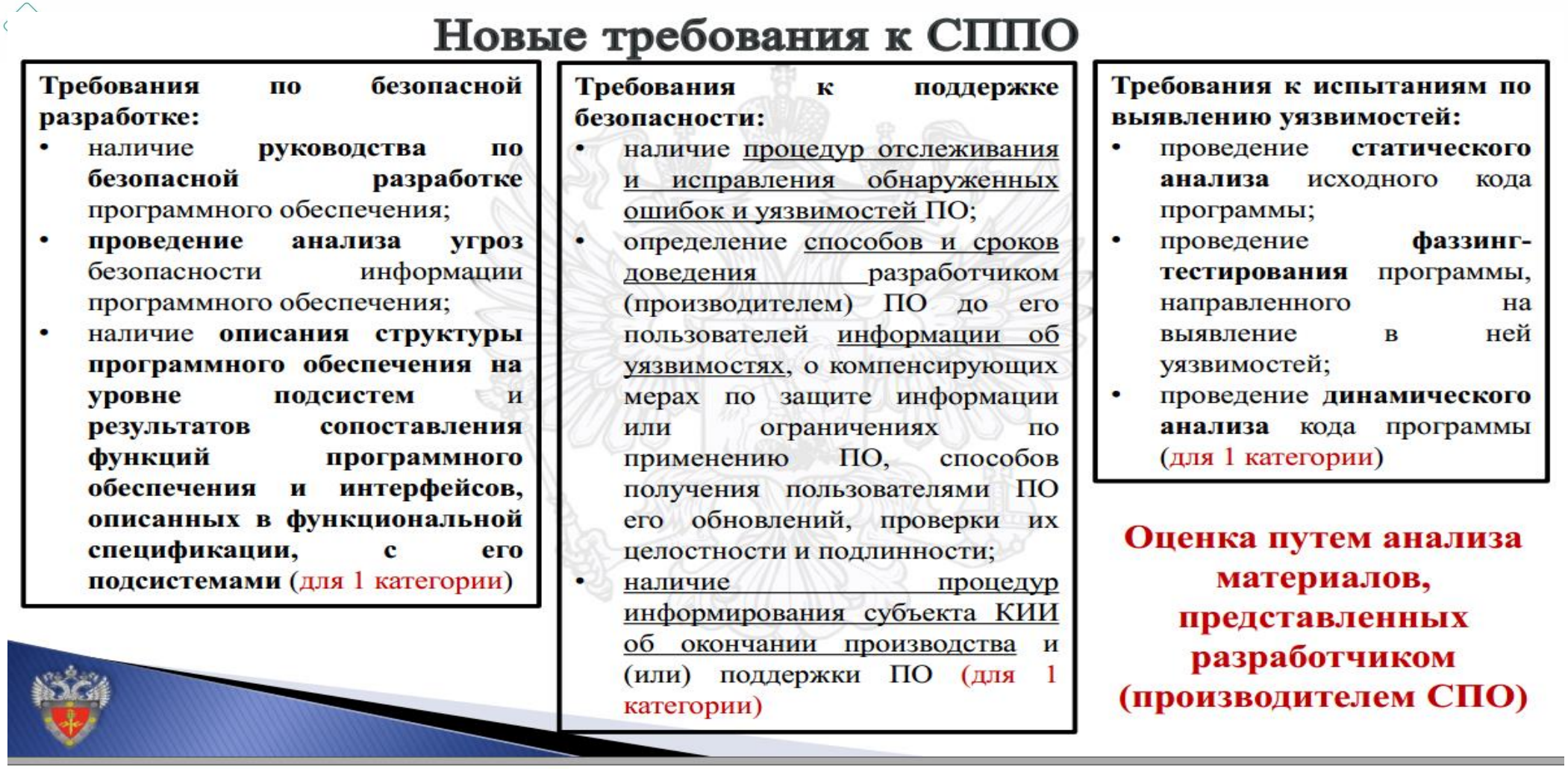






- Проверка документации.
- Проверка комплекта поставки.
- Разработка безопасного программного обеспечения.
- Поддержка безопасности поставляемого программного обеспечения.
- Проверка отсутствия уязвимостей и НДВ программного обеспечения и баз данных.
- Организационно-технические требования к эксплуатации.

Реализация организационно-технических требований



СПО – специальное прикладное программное обеспечение

Инструментальное ПО для испытаний по выявлению уязвимостей

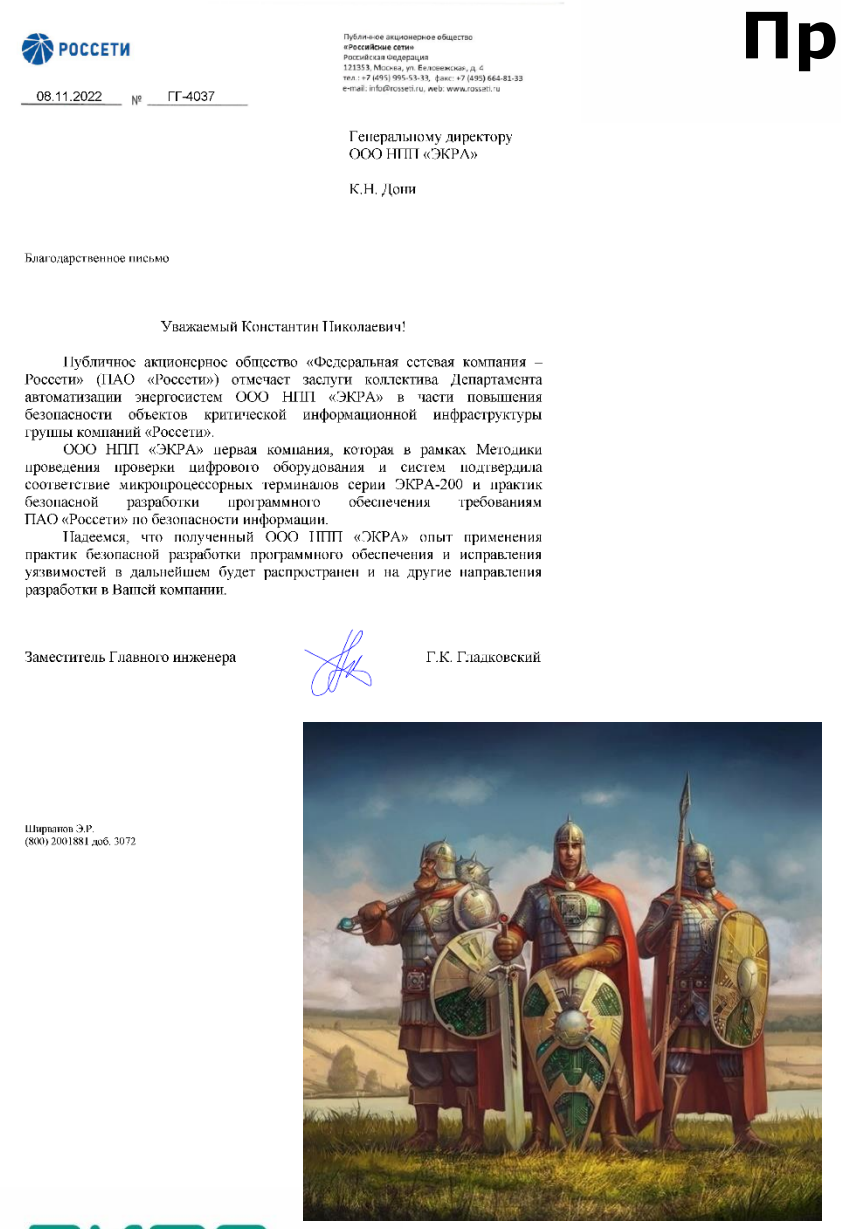
Инструменты статического анализа

- Solar appScreener
- PVS-Studio
- Svace
- FxCop
- StyleCop
- Duplicates Finder (.Net)
- Cppcheck

Инструменты динамического анализа и фаззинг-тестирования

- MS Visual Studio
- PerfMon
- Process Explorer
- ANTS Memory Profiler
- .Net Memory Profiler
- Утилиты компании JetBrains (DotTrace, DotMemory, DotCover)
- Application Verifier
- Блесна
- ИСП Crusher

Сложности реализации. Промежуточные выводы



РОССЕТИ

Публичное акционерное общество
«Российские сети»
Российская Федерация
121353, Москва, ул. Беловежская, д. 4
тел.: +7 (495) 995-55-33, факс: +7 (495) 664-81-33
e-mail: info@rosseti.ru, web: www.rosseti.ru

08.11.2022 № ГГ-4037

Генеральному директору
ООО НПП «ЭКРА»

К.Н. Дони

Благодарственное письмо

Уважаемый Константин Николаевич!

Публичное акционерное общество «Федеральная сетевая компания – Россети» (ПАО «Россети») отмечает заслуги коллектива Департамента автоматизации энергосистем ООО НПП «ЭКРА» в части повышения безопасности объектов критической информационной инфраструктуры группы компаний «Россети».

ООО НПП «ЭКРА» первая компания, которая в рамках Методики проведения проверки цифрового оборудования и систем подтвердила соответствие микропроцессорных терминалов серии ЭКРА-200 и практик безопасной разработки программного обеспечения требованиям ПАО «Россети» по безопасности информации.

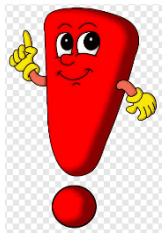
Надеемся, что полученный ООО НПП «ЭКРА» опыт применения практик безопасной разработки программного обеспечения и исправления уязвимостей в дальнейшем будет распространен и на другие направления разработки в Вашей компании.

Заместитель Главного инженера Г.К. Гладковский

Ширапов Э.Р.
(800) 2001881 доб. 3072

Для успешного прохождения оценки соответствия **нам потребовалось**:

- ✓ **Доработка** внутреннего и прикладного ПО и внедрение встроенных средств защиты информации.;
- ✓ Внесение объекта оценки в **реестр российского ПО** и обеспечение эксплуатации ПО, с использованием в составе компонентов ПО, включенных в реестр российского ПО;
- ✓ Обеспечение **импортозамещения** электронной компонентной базы;
- ✓ **Отказ от небезопасных сетевых протоколов** (FTP, Telnet, Http и другие) и отключение в проектах неиспользуемых интерфейсов;
- ✓ Выполнение **испытаний по выявлению** уязвимостей и недекларированных возможностей в ПО;
- ✓ **Реорганизация внутренних бизнес-процессов** на предприятии, в т.ч. внедрение технологий жизненного цикла разработки безопасного ПО;
- ✓ Повышение квалификации сотрудников для проведения статического и динамического анализа, фаззинг-тестирования ПО: ИСП РАН и ФСТЭК, и др. (очно и онлайн).



И главное: обзавестись “словарем” терминов по ИБ чтобы они стали понятны релейщикам и специалистам по разработке ПО !
Требуется переход от “стереотипных” знаний по ИБ к вполне понятным и однозначно трактуемым требованиям .

ЭКРА

Технические решения по ИБ для энергообъектов.

Принципиально все средства ИБ можно разделить на три группы:

- Встроенные средства (рассмотрены в презентации ранее на примере РЗА);
- Наложенные средства (межсетевые экраны, антивирусы, система обнаружения вторжений и т.д.);
- Организационные (мероприятия которые позволяют повысить уровень ИБ организационными методами).

Мы делаем технические решения по ИБ энергообъектов “под ключ” совместно с решениями партнеров.

В настоящее время занимаемся реализацией средств ИБ по всей номенклатуре продукции “ЭКРА”.

ЭКРА

Технические решения по ИБ для энергообъектов.

1. Не бывает **абсолютной защиты и абсолютной безопасности**;

2. Идет постоянная борьба “меча” и “щита”. Но **где фактические статистические данные про российские компании ?** Их в доступных источниках нет – все остальное это манипуляции данными без ссылок на первоисточники.

3. Предлагаемый и декларируемый **путь стандартизации оборудования и технических решений по ИБ** только лишь упрощает задачу взлома объектов. Типовые и единые решения по ИБ для всех энергообъектов = **типовая модель взлома любого энергообъекта** !

4. Можно **стандартизировать МИНИМАЛЬНЫЕ требования** к функционалу ИБ, но **не требования к их реализации**. В противном случае получаем крайне уязвимую систему.

Технические решения по ИБ для энергообъектов.

5. Все чаще **требования к ИБ** предъявляются к вторичному оборудованию энергообъектов (преимущественно к РЗА) **путем переноса требований с наложенных средств ИБ**;
Это существенно повышает требования к производительности применяемых чипов, а в конечном итоге все вторичное оборудование сильно дорожает.

6. **Избыточный функционал** предъявляемый только к РЗА приводит не только к удорожанию, но и **снижению показателя надежности** и повышению времени готовности устройства.

7. [перенос требований на РЗА по п.5] удаляет нас от возможности использовать отечественные чипы и ЭКБ, произведенную в РФ. **Заставляет переходить на иностранные чипы** с высокими требованиям по производительности и телекоммуникационным возможностям - это преимущественно **решения из США**. Это точно безопаснее ? (ближайшие 10 лет отечественных чипов под эти требования не будет)

ЭКРА

Технические решения по ИБ для энергообъектов.

8. Все чаще идет **подмена понятий** информационной безопасности и физической безопасности – границы размываются.
👉 пример 1: угроза в периметре (нарушитель на объекте) и взламывает терминал РЗА для нарушения электроснабжения;
👉 пример 2: угроза в периметре и взламывает цифровую сеть МЭК 61850 для нарушения электроснабжения;
👉 пример 3: угроза в периметре и взламывает SCADA систему управляющую электроснабжением;
👉 пример 4: и т.д;

Что бы сделал я попав в периметр как специалист:
1) проводом в 1-1,5м (“закоротка”) в шкафах УПАСК и ДЗШ отключил бы электроснабжение на ПС где нахожусь, а также путем пусков команд УПАСК нарушил бы электроснабжение всех объектов вокруг.
2) А если все по МЭК 61850 ? Нашел бы ПДС и все сделал через них !
3) Это нормально если я со стороны оказался здесь ? При проектировании все больше говорят про ИБ без физической безопасности объекта (либо просто формальный подход). Рубль вложенный в физич.безопасность сэкономит несколько рублей из ИБ безопасности.

ЭКРА

Технические решения по ИБ для энергообъектов.

9. **Шифрование всего и вся** в пределах защищаемого контура – требуется определить границы разумного (предлагается вводить шифрование всего трафика, при этом никто не задается вопросом “а кто же отправил этот GOOSE” ?).

10. Внедрение общих **гигабитных шин без сегментации сетей** на ЦПС по МЭК 61850 снижает требования к надежности РЗА. Устройство РЗА перестает быть устройством РЗА с требованиями обеспечивающими гарантированное отключение при КЗ, в т.ч., например, при пропадании питания на энергообъекте.

11. Может ли защита (система ИБ) быть **сопоставима со стоимостью основных средств** управления ? В ряде проектов уже похоже что да !

12. Не всегда прослеживается **взаимосвязь и увязка** средств встроенной ИБ и наложенных средств ИБ, а тем более средств физической безопасности. **Проверка корректности настройки и совместимости** средств ИБ.

Хотите знать больше про нашу продукцию, а также её соответствие международным, корпоративным требованиям, а также требованиям по информационной безопасности ?

https://ekra.ru/company/news/

https://t.me/npp_ekra/

Разумов Роман Вадимович
Директор департамента автоматизации энергосистем

razumov_rv@ekra.ru
8(8352)220-110 доб.1374
8(919)666-73-10

ЭКРА

СПАСИБО ЗА ВНИМАНИЕ!