Решения SEL по кибербезопасности

Практичные, управляемые, масштабируемые решения

Кибербезопасность нельзя обеспечить усилиями одного человека, использованием одного продукта или технологии. Настоящая защита в масштабе всей системы начинается с понимания того, что для достижения успеха необходима командная работа. Мы в компании SEL считаем, что создание безопасного и соответствующего нормативным требованиям решения - это комбинация многоуровневой безопасности и усилий инженеров по системам защиты, IT персонала и менеджеров по обеспечению соответствия.

Защита энергосистемы

Инженерам-энергетикам нужны самые надежные системы и услуги для систем управления и защиты. Уставки не должны сбиваться, кабели - отключаться, а чрезмерная задержка недопустима. Инженеры должны иметь возможность осуществлять полное управление важными системами и доступом к оборудованию 24 часа в сутки, 365 дней в году. Кибербезопасность должна обеспечивать защиту данных активов и давать возможность инженерам эффективно выполнять свою работу.

Информационные технологии (IT).

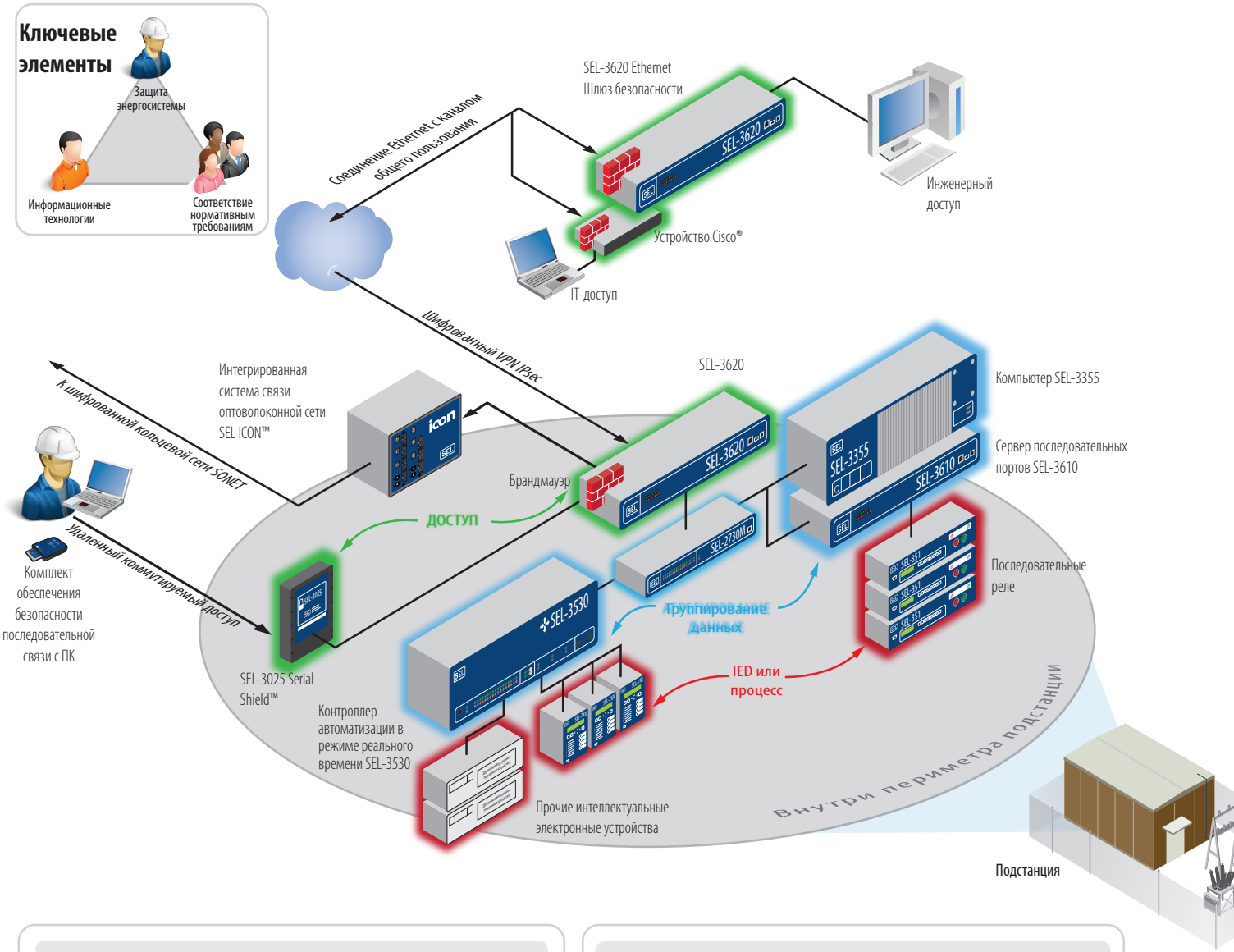
IT-персонал понимает как работать в крупной, динамичной сетевой среде. Эксперты компании SEL знают, что необходимо, чтобы контролировать свою среду, защищать серверы и клиентов, а также предоставлять наилучшие возможные технологические услуги для своей организации. IT-персоналу необходимы решения, которые совместимы с их инфраструктурой, и которые расширяют возможности за счет упрощения работы.

Соблюдение нормативных требований

Менеджерам по обеспечению соответствия необходимы устройства, которые обеспечивают соответствие стандартам CIP NERC, сейчас и в будущем. Это требует реализации масштабируемых решений, которые управляются централизованно. Соответствие нормативным документам является сложной и необходимой работой. В дополнение к обеспечению соответствующей функциональности, технологии должны собирать и представлять точные данные, позволяющие облегчить процесс соблюдения нормативных требований.

Повышение безопасности, надежности и экономичности энергоснабжения®

Решения системной безопасности SEL



Масштабируемость

Компания SEL создает безопасность на системном уровне. Мы создаем управляемые, масштабируемые решения, которые помогают управлять системой, независимо от количества подстанций - будь то одна или несколько сотен подстанций.

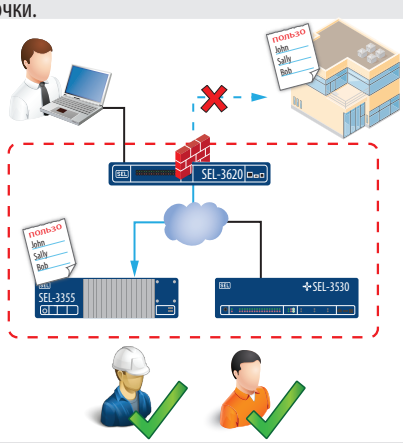
Зона 1: Доступ
Надежное управления доступом для защиты данных Ethernet и последовательных данных при входе/выходе из существующего периметра эл. безопасности (ESP). Создание прокси-модуля для устройств предыдущих поколений повышает безопасность без обновления прошивки.

Зона 2: Группирование данных
Обеспечение строгого управления доступом через службу безопасности на уровне портов, настраиваемые уровни доступа к локальному и удаленному доступу, строгая аутентификация и защищенные протоколы.

Зона 3: IED или процесс
Предоставление пользовательского и административного доступа с надежными паролями, включением/отключением портов, и контактами сигнализации, информирование соответствующих систем о событиях или изменениях в настройках.

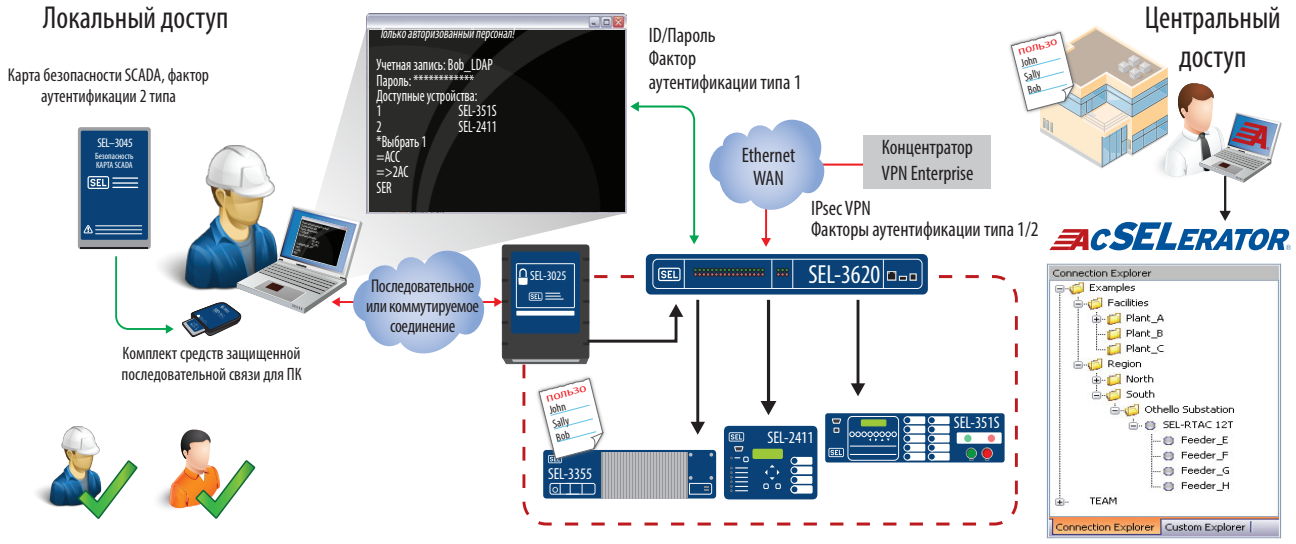
Централизованная аутентификация и высокая доступность

Права и разрешения пользователей дублируются при помощи компьютера SEL-3355 работающего под управлением Windows Server® 2008. Это позволяет персоналу сохранить обычный доступ к подстанции, если канал связи с основным сервером Microsoft® Active Directory® недоступен. Доступ и права аутентификации настраиваются из одной точки.



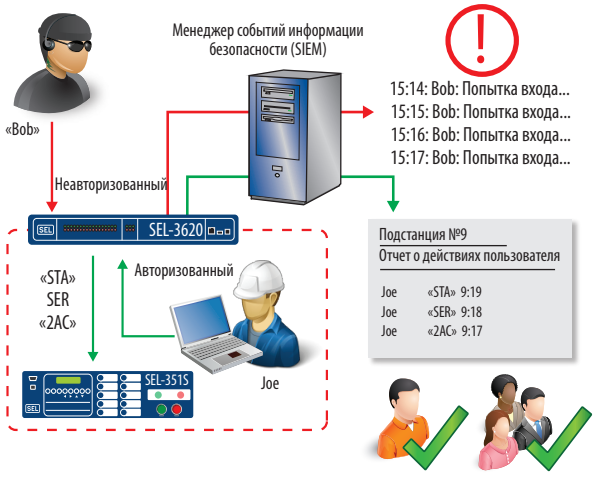
Централизованная аутентификация

Получение интерактивного доступа посредством защищенной электронной точки доступа (EAP) к удаленному периметру электронной безопасности (ESP), используя централизованные данные прокси-серверов шлюза безопасности Ethernet SEL-362. Авторизованные пользователи могут получить доступ к IED без необходимости запоминать отдельные логины реле. В командировке, в офисе или на территории подстанции пользователи могут использовать соответствующие приложения для конфигурирования в командной строке или программное обеспечение acSELerator QuickSet® SEL-5030 с графическим интерфейсом пользователя (GUI), позволяющим вносить изменения, просматривать события или проверять информацию о состоянии.



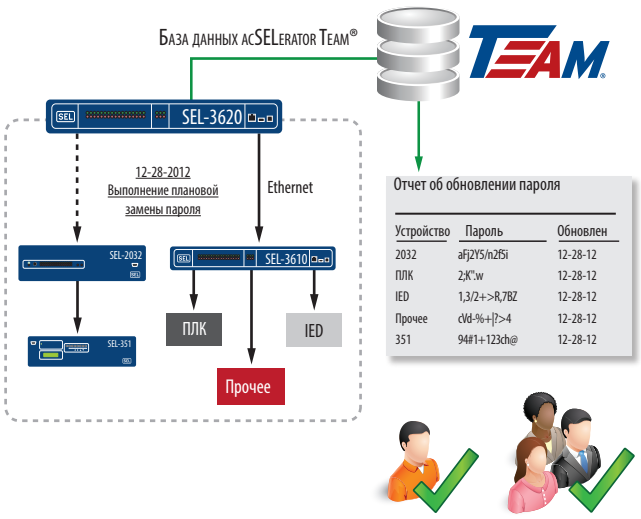
Идентифицируемость пользователей и соответствие требованиям безопасности

Интеграция в существующие системы управления журналами событий осуществляется по протоколу Syslog. Хранение журналов вне площадки способствует упрощению процесса соответствия правилам и нормативным документам по регистрации событий инфраструктуры NERC CIP. Прокси-сервисы шлюза безопасности Ethernet SEL-3620 обеспечивают генерацию отчетов о выполнении команд пользователя и отслеживают все действия, выполняемые на электронных устройствах (IED) отдельными пользователями..



Автоматическое управление паролями электронных устройств (IED)

Прокси-сервисы SEL-3620 обеспечивают быстрое и эффективное управление паролями IED. На IED устанавливаются надежные пароли, которые автоматически изменяются по настраиваемому графику, при этом обеспечивается, чтобы в сетях критической важности не использовались пароли по умолчанию или ненадежные пароли.



Продукты обеспечения безопасности компании SEL разработаны для обеспечения надежного энергоснабжения, и повышают удобство и упрощают работу в системе в целом. Мы понимаем необходимость обеспечения высокой степени надежности и доступа в режиме реального времени ко всем критически важным работам. Наши устройства являются масштабируемыми и взаимодействуют с IT-инфраструктурой. Надежная безопасность и соответствие стандартам - это не продукт выполнения нормативных актов, а результат прогнозирования, планирования и добросовестной практики безопасности.

Решения SEL по кибербезопасности



Функциональная потребность	**SEL-3620** Шлюз безопасности Ethernet	**SEL-3025** Serial Shield™		**Компьютер** SEL-3355	**SEL-5045 программное обеспечение** acSELerator Team®*
		Опция: протокол поточного шифрования (SEP)	**Опция: безопасный протокол связи SCADA (SSCP)**		
Безопасная сеть SCADA	Шифрование всего Ethernet-трафика и Ethernet-инкапсулированных последовательных данных, передающихся через медные или оптоволоконные линии связи Ethernet с широкими возможностями IPsec VPN, брандмауэра и Secure Shell (SSH).	Обеспечение безопасности последовательной связи SCADA, в том числе всех байт-ориентированных протоколов и большинства бит-ориентированных протоколов с очень низкой задержкой.	SEL-3620 или SEL-3025 (опция).	SEL-3620 или SEL-3025 (опция).	SEL-3620 или SEL-3025 (опция).
Безопасный коммутируемый (Dial-Up) доступ	В комбинации с SEL-3025 опция SSCP и комплект обеспечения безопасности последовательной связи с ПК (PC Serial Security Kit) предоставляют дополнительные возможности аутентификации.	Опциальный вариант SEL-3025 SSCP и комплект безопасности последовательной связи с ПК.	Обеспечение безопасности коммутируемых (Dial-Up) соединений с криптографическим шифрованием по стандарту FIPS 140-2 уровень 2, при конфигурации с SSCP и комплектом безопасности последовательной связи с ПК.	Опциальный вариант SEL-3025 SSCP и комплект безопасности последовательной связи с ПК.	Опциальная функция управления удаленными устройствами через коммутируемое соединение, безопасность которого обеспечивается SEL-3025 SSCP и комплектом безопасности последовательной связи с ПК.
Инженерный контроль доступа с высоким уровнем надежности	SEL-3620 можно использовать в качестве электронной точки доступа (EAP), которая определяет электронный периметр безопасности (ESP). Предоставление единой точки входа для важных интеллектуальных электронных устройств (IED) с последовательным и Ethernet-подключением с контролем доступа пользователей. Пользователям требуется запомнить только имя учетной записи и пароль.	SEL-3620 или SEL-3025 SSCP (опция).	Прозрачное шифрование и аутентификация всех интерактивных инженерных сеансов коммутируемого доступа к удаленному устройству SEL-3025 при использовании комплекта безопасности последовательной связи с ПК. В сочетании с SEL-3620 обеспечивается реальная двухфакторная аутентификация для коммутируемых соединений.	Обеспечение резервируемой централизованной аутентификации учетных записей пользователей и паролей на всем предприятии при использовании Windows Server 2008 с доменными службами Microsoft Active Directory. Обеспечение резервирования доступа в случае отказа линии связи с центральным сервером.	SEL-3620 или SEL-3025 SSCP (опция).
Централизованное управление	Обеспечение безопасного управления с удаленного компьютера с помощью HTTPS и/или программного обеспечения acSELerator TEAM Software. Установка сильных паролей реле при помощи автоматизированного управления паролями электронных устройств (IED).	Обеспечение безопасного управления с удаленного компьютера с помощью HTTPS или безопасного последовательного соединения.	Обеспечение безопасного управления с удаленного компьютера с помощью HTTPS, безопасного последовательного соединения или программного обеспечения acSELerator TEAM.	Поддержка централизованного управления учетными записями и паролями предприятия. Настройка из одного места прав авторизации и запрета доступа. Изменения автоматически синхронизируются с контроллерами домена подстанции.	Автоматическое управление локальными и удаленными продуктами SEL в полях через Ethernet, последовательное или коммутируемое соединение.
Идентифицируемость пользователей и поддержка обеспечения соответствия требованиям стандартов безопасности	Формирование отчетов об активности пользователей (Syslog и PDF для себя, PDF для подключенного электронного устройства IED), включая доступ и действия по изменению, выполняемые отдельными пользователями. Обеспечение строгого контроля безопасности и доступа в электронный периметр безопасности (ESP).	Реализация средств строгого контроля доступа, а также регистрация всех изменений и попыток доступа из SCADA сети при помощи Syslog.	Реализация средств строгого контроля доступа, а также регистрация всех изменений и попыток доступа из сети коммутируемого доступа при помощи Syslog.	Сбор, хранение и передача журналов событий при помощи Syslog. Также возможна реализация в качестве локального коллектора Syslog для защищаемых устройств.	Опциальная функция опроса продуктов безопасности SEL, и сбор журналов и отчетов для централизованного хранения и управления.

Университет SEL (SELU)

SEL предлагает курсы по информационной безопасности и сетям SCADA, включая COM 203: Передовые практики SEL по обеспечению информационной безопасности важных инфраструктур (SEL Cybersecurity Best Practices for Critical Infrastructure). Мы также предлагаем новый курс, APP 3620: Шлюз безопасности Ethernet.

ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ УСЛУГИ

Команда подразделения инженерно-технических услуг Engineering Services SEL также предлагает услуги по испытанию функционирования и устройства системы безопасности. Услуги включают испытания на проникновение, сканирование уязвимостей, испытания аудита соответствия NERC CIP и многое другое.

Pullman, Washington, США
Тел.: +1.509.332.1890 • Факс: +1.509.332.7990 • www.selinc.com • info@selinc.com