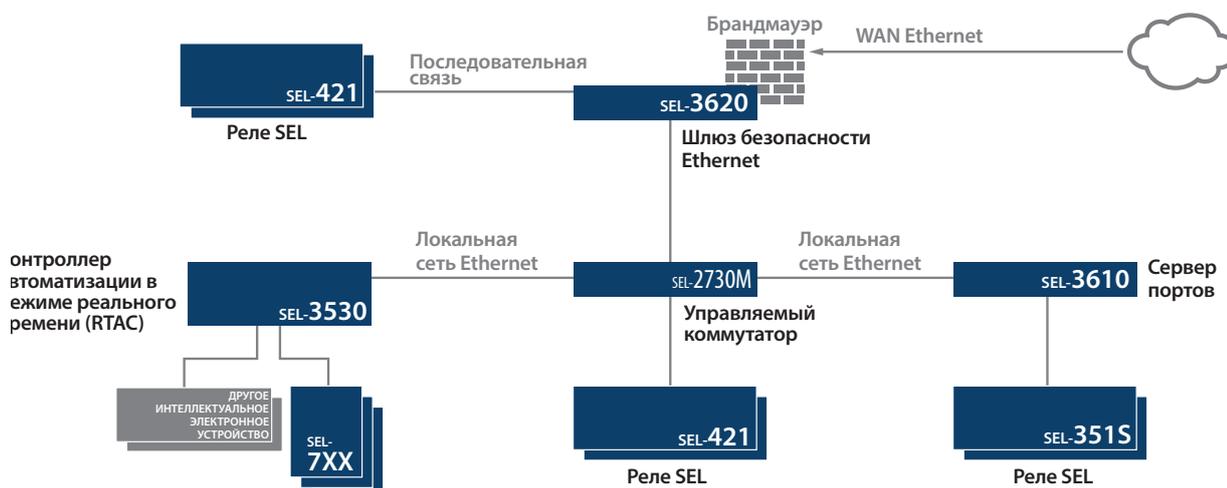


SEL-3620

ШЛЮЗ БЕЗОПАСНОСТИ ETHERNET



МОЩНЫЙ КОНТРОЛЬ ДОСТУПА В ПЕРИМЕТР ЭЛЕКТРОННОЙ ЗАЩИТЫ



ГЛАВНЫЕ ОСОБЕННОСТИ

Централизованный доступ к реле и ИЭУ

Шлюз безопасности SEL-3620 используется для создания централизованной точки доступа к важнейшим цифровым активам и обеспечивает средства контроля доступа пользователей и ведение подробных журналов операций. Таким образом, авторизация проходит через шлюз безопасности SEL-3620, а не через отдельные интеллектуальные электронные устройства (ИЭУ). Централизованное управление учетными записями пользователей и групповым членством происходит с помощью систем, доступных по протоколу LDAP, таких как служба Microsoft® Active Directory®. Дополнительная Служба коммутируемого доступа для удаленных пользователей (RADIUS) позволяет использовать системы многофакторной проверки подлинности, такие как токены RSA.

Встроенное антивирусное программное обеспечение с «белым списком»

Защита от известных и неизвестных вредоносных атак на шлюзы безопасности SEL обеспечивается с помощью встроенного антивируса eXe-GUARD™. Мощная технология защиты от руткитов, встроенные средства обязательного контроля доступа Linux® и «белый список» процессов помогают справиться с атаками на сами шлюзы и устранить дорогостоящее управление исправлениями и необходимость обновления баз антивирусных программ.

Брандмауэр подстанции и конечная точка IPsec VPN

Защита сети подстанции от вредоносного трафика осуществляется с помощью мощного брандмауэра, блокирующего подозрительный трафик по умолчанию. Управление состоянием и конфигурацией происходит через интуитивный интерфейс, активируемый через меню. Критически важные сети безопасно подключаются к центру управления посредством технологии виртуальной частной сети (VPN) и пакета протоколов Internet Protocol Security (IPsec). Для централизованного управления доверием используются сертификаты X.509 с протоколом OCSP. Шлюз безопасности SEL-3620 совместим с устройствами с поддержкой Lemnos®.

Мощные средства контроля и создание отчетов о действиях пользователей

Шлюз регистрирует факт и время доступа пользователей и всех команд, поданных на критически важные ИЭУ. Записи о событиях интегрируются с существующими системами управления журналами при помощи стандарта Syslog. Защита ИЭУ осуществляется надежными паролями, при этом блокируются общие и создаваемые по умолчанию учетные записи. Детальные средства контроля доступа ограничивают доступ пользователей к назначенным ролям на отдельных ИЭУ.

Управление паролями ИЭУ

Установка надежных паролей на ИЭУ и их автоматическое изменение по настраиваемому расписанию. Выполнение нормативных требований к паролям и недопущение использования ненадежных или по умолчанию устанавливаемых паролей. Управление паролями на ИЭУ с интерфейсом командной строки и на устройствах, работающих по протоколу Modbus® (например, на последовательных реле GE UR).

Поддержка требований стандарта NERC CIP

SEL-3620 обеспечивает мощный контроль доступа пользователей к периметру электронной защиты (ESP), защиту ИЭУ надежными паролями и блокировку совместных учетных записей и учетных записей, создаваемых по умолчанию. Детальные средства контроля доступа ограничивают доступ пользователей назначенными ролями на отдельных ИЭУ. Все действия пользователей фиксируются, и операторы системы на удаленных объектах оперативно получают сигналы предупреждения через журналы Syslog.

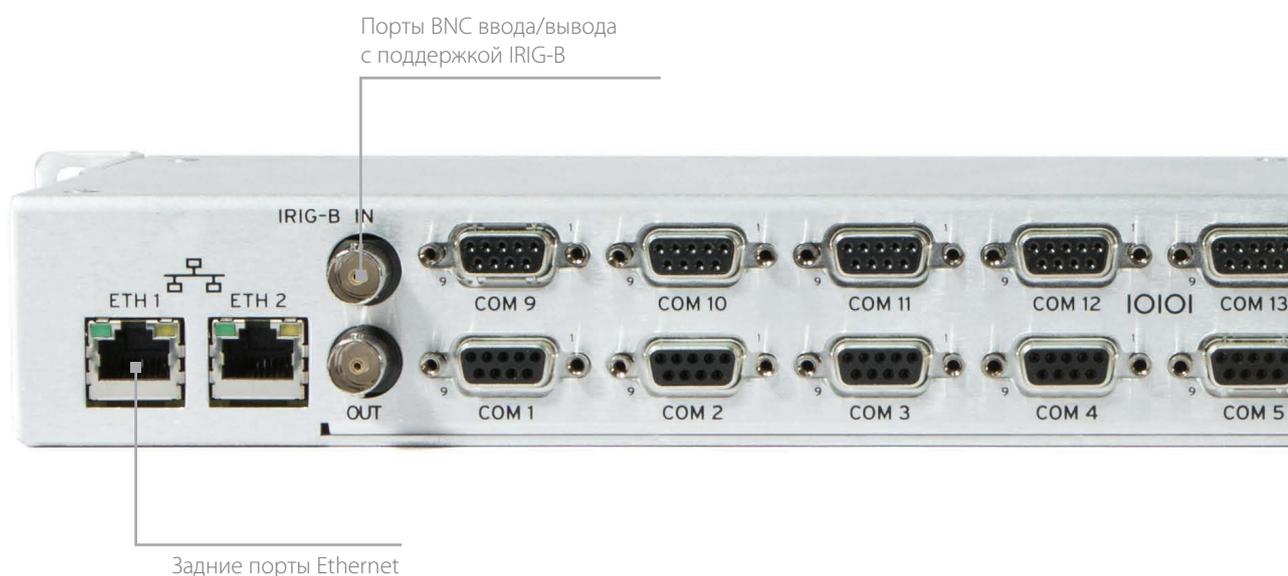
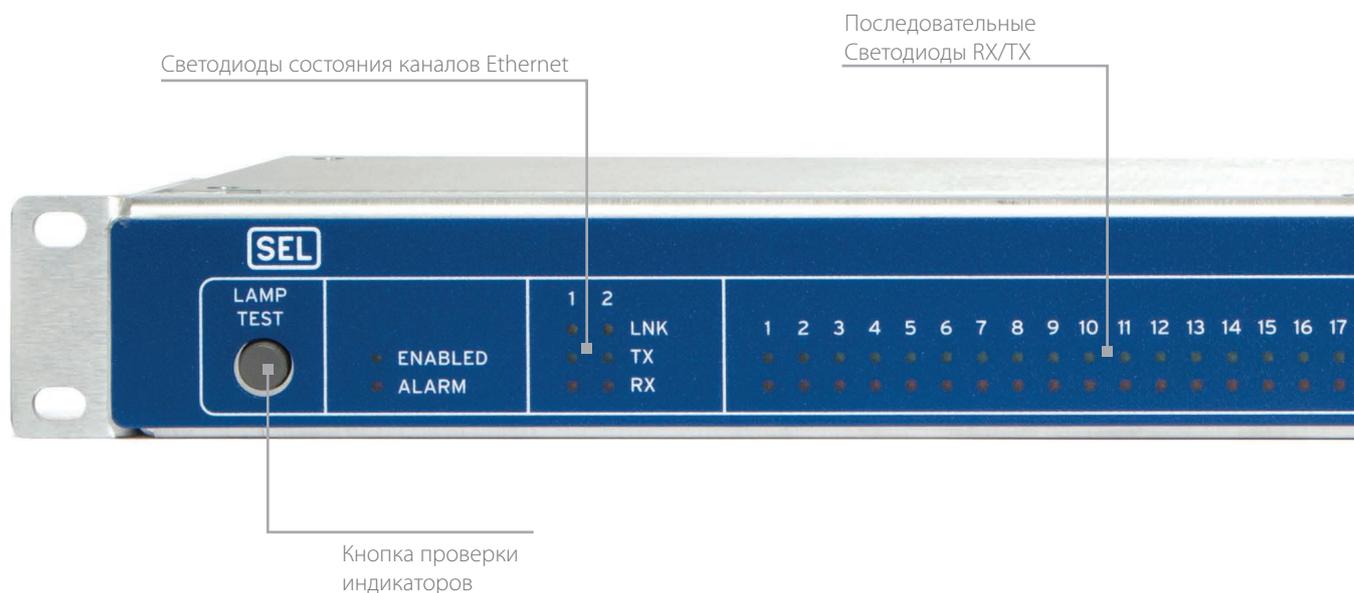
Приемопередатчик с последовательного порта на Ethernet

Расширение совместимости протоколов путем оперативного перевода последовательных DNP3 и Modbus® в Ethernet DNP3, протокол управления передачей (TCP) и Modbus TCP. Создание подключения Ethernet, используя Secure Shell (SSH), Telnet, или инкапсуляцию Raw TCP для создания постоянного канала между логическим портом Ethernet и физическим последовательным портом.

Поддержка виртуальных программных клиентов

С помощью клиента Virtual Connect SEL-5827 или программы SEL-5828 Virtual Port Service можно модернизировать криптографической защитой незащищенные последовательные каналы связи и существующие каналы связи Ethernet на компьютерах под управлением Windows®. Эти функции бесплатно предоставляются SEL для использования удаленных портов SEL-3620 с существующими программами и терминалами на ПК, в том числе с теми из них, которые используют Modbus TCP/RTU. Защита данных обеспечивается протоколом SSH на группах портов, ведущих (master) и последовательных портах SEL-3620.

ОБЗОР ПРОДУКТА



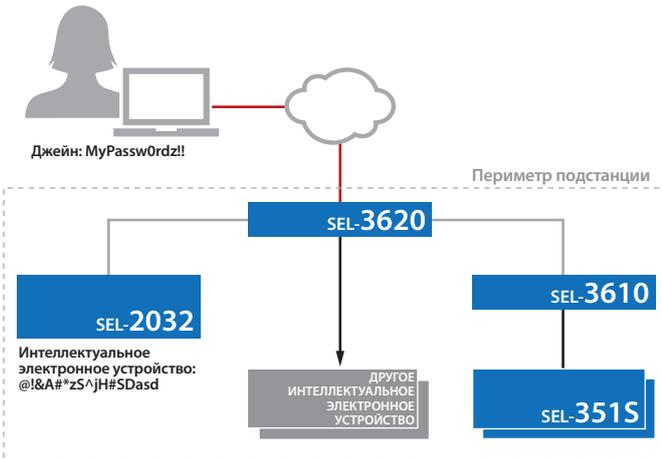


ОБЛАСТИ ПРИМЕНЕНИЯ

РАЗУМНЫЕ, УПРАВЛЯЕМЫЕ, МАСШТАБИРУЕМЫЕ РЕШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

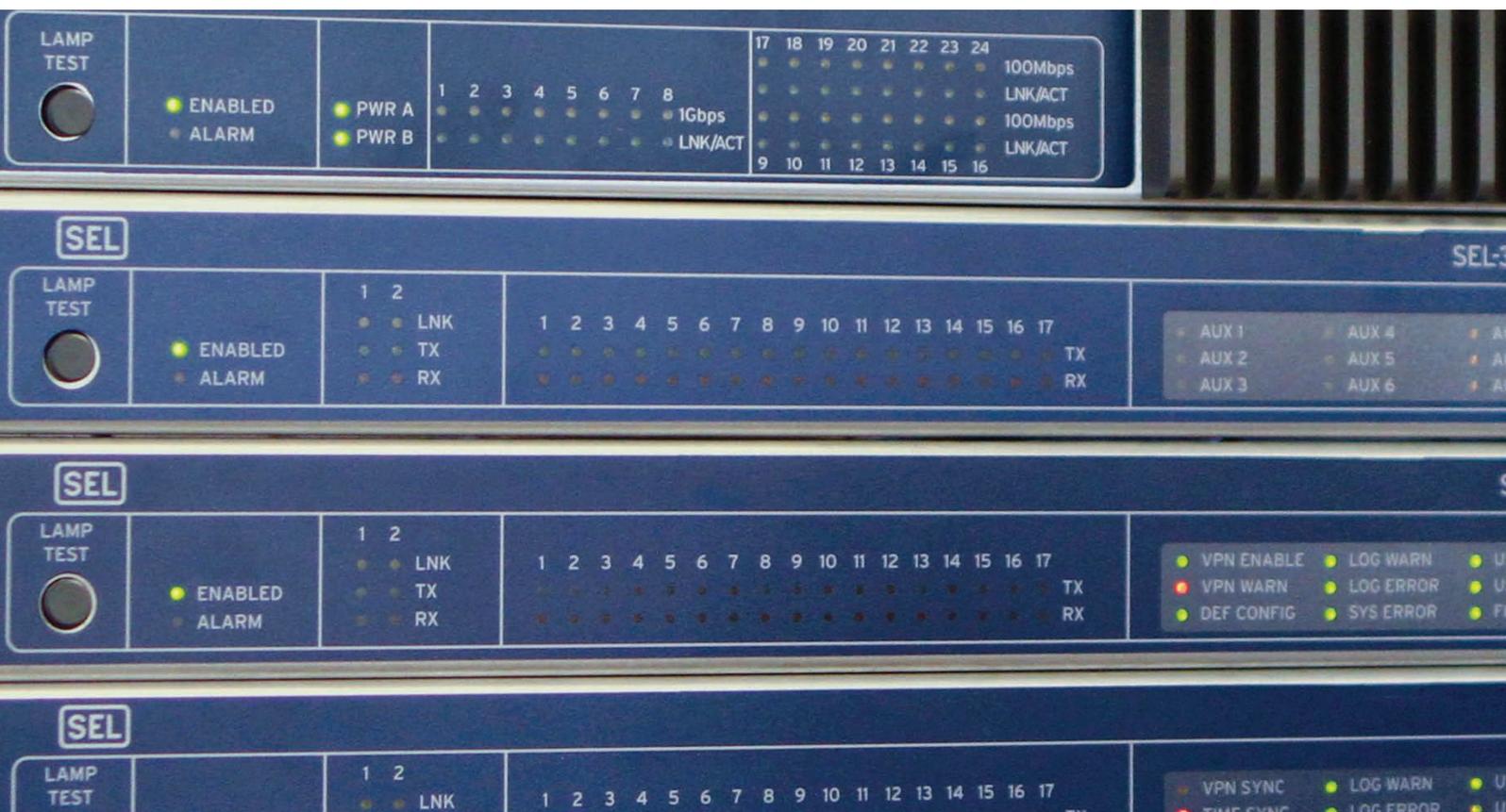
Управление защитой устройств с помощью надежных паролей

Шлюз безопасности SEL-3620 обеспечивает быстрое и эффективное управление паролями ИЭУ. Для ИЭУ используются надежные пароли, которые автоматически изменяются по заданному расписанию, при этом в критически важных сетях не используются пароли по умолчанию или слабые пароли. Пользователям нужно знать только свои собственные пароли, а не пароли ИЭ.



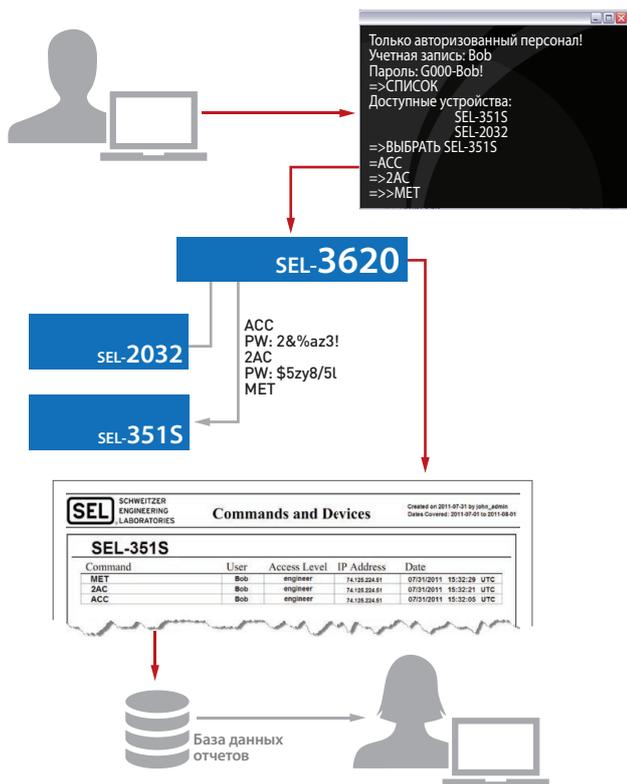
Управление доступом пользователей

Запрос в Microsoft Active Directory осуществляется с использованием LDAP или RADIUS. Администраторы системы могут легко добавлять и исключать учетные записи пользователей для доступа и авторизовать уровни доступа для отдельных устройств с центральной станции.



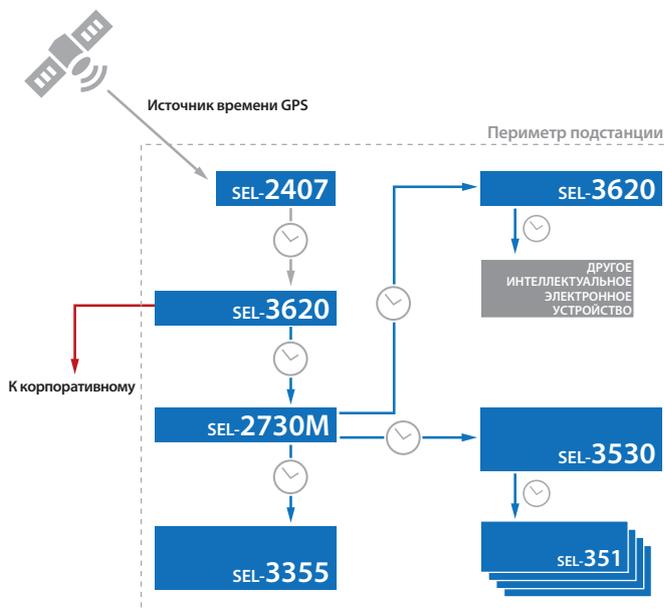
Отчеты о действиях пользователей

SEL-3620 позволяет создавать подробные отчеты, в которых фиксируются отдельные пользователи и команды, поданные ими на ИЭУ, а также все действия пользователей, выполняемые ими на защищенных устройствах. Пользователи, имеющие соответствующие права, могут загружать отчеты о подключениях, что позволяет выполнять подробный анализ и действий пользователей и обеспечивает их максимальный контроль.



Синхронизация времени

SEL-3620 обеспечивает синхронизацию времени всех защищенных ИЭУ, концентраторов данных и промышленных вычислительных устройств. Для распределения данных точного времени используются протоколы IRIG-B и протокол сетевого времени (NTP) на основе Ethernet. При временном отключении спутникового источника времени SEL-3620 поддерживает сигналы точного времени на подстанции при помощи собственных внутренних часов.





**ПОВЫШЕНИЕ БЕЗОПАСНОСТИ, НАДЕЖНОСТИ
И ЭКОНОМИЧНОСТИ ИСПОЛЬЗОВАНИЯ
ЭЛЕКТРОЭНЕРГИИ**

SCHWEITZER ENGINEERING LABORATORIES, INC.

Тел.: +1 (509) 332-18-90

Эл. почта: info@selinc.com

Веб-сайт: www.selinc.com

