

# Криптографическая защита без компромиссов

*Директор ООО «Эс-Крипто» Валерий Вижукайло*

При создании информационных систем, предназначенных для обработки информации, распространение которой ограничено, остро стоит вопрос защиты такой информации. Особенностью защиты информации является нахождение баланса между удобством пользования информационной системой, снижением затрат на ее администрирование и точное выполнение требований законодательства Республики Беларусь.

Для обеспечения требований законодательства Республики Беларусь по криптографической защите информации в информационных системах и обеспечения пользователей средствами криптографической защиты компанией ООО «Эс—Крипто» разработана линейка продуктов под брендом **S-Crypto VPN**.

Все продукты комплекта S-Crypto VPN имеют сертификаты соответствия техническому регламенту Республики Беларусь ТР 2013/027/ВУ и соответствуют требованиям СТБ 34.101.27-2022 для различных уровней безопасности.

**S-Crypto VPN** решает сразу несколько задач:

- построение защищенных виртуальных частных сетей;
- управление информационными потоками;
- фильтрация и контроль сетевого трафика;
- обеспечение криптографической защиты в соответствии с нормативными требованиями.

## **Архитектура решения: от серверного уровня до пользовательских устройств**

Линейка S-Crypto VPN выстроена как целостная экосистема, охватывающая все уровни взаимодействия. В центре архитектуры находится **S-Crypto VPN Server**, который выступает ядром системы. Он формирует защищенные каналы связи на базе технологии VPN-TLS и одновременно выполняет функции межсетевого экрана. С точки зрения эксплуатации это дает предсказуемый результат — решение справляется с высоконагруженными сценариями (до 15 Гбит/с), поддерживает различные методы аутентификации, включая двухфакторную, и позволяет безопасно администрировать инфраструктуру через доверенные каналы.

## **Клиентский уровень: безопасность без усложнения**

На уровне конечного пользователя ключевую роль играет **S-Crypto VPN Client**. В данном случае акцент сделан на прозрачности работы: клиент поддерживает подключение к нескольким VPN-серверам, автоматически восстанавливает соединение и адаптирует интерфейс под уровень пользователя — от базового до продвинутого. Это снижает зависимость от ИТ-службы и сокращает количество инцидентов, связанных с человеческим фактором.

## **Централизованное управление как основа масштабирования**

В распределенной инфраструктуре вопрос управления становится критичным. Для этого в линейке предусмотрен **S-Crypto VPN Server Manager** — инструмент, который позволяет администратору работать не с отдельными узлами, а с системой в целом. Фактически речь

идет о единой точке контроля, через которую можно управлять множеством серверов, отслеживать конфигурации и поддерживать единую политику безопасности. Важно, что администрирование также осуществляется через защищенные каналы, что исключает появление уязвимостей на уровне управления.

### **Аппаратно-программный контур: защита для критических систем**

Для сценариев с повышенными требованиями к безопасности, включая системы класса 3-ДСП, предусмотрен программно-аппаратный комплекс **S-Crypto VPN 1.0**. В отличие от чисто программных решений, здесь безопасность закладывается на уровне всей платформы. Комплекс включает преднастроенную операционную систему S-Crypto OS, встроенные механизмы фильтрации трафика и соответствует более высокому уровню требований (уровень 3 СТБ).

### **Мобильный доступ как часть корпоративной безопасности**

С ростом мобильных сценариев работы защита должна распространяться и на пользовательские устройства. **S-Crypto VPN Client для Android** решает эту задачу без необходимости использования дополнительного оборудования.

Ключевые функции остаются теми же, что и в десктопной среде: двухфакторная аутентификация, автоматическое восстановление соединения и соответствие требованиям безопасности. Это позволяет включать мобильных сотрудников в защищенный контур без снижения общего уровня защиты.

### **Практика внедрения**

На сегодняшний день решения S-Crypto VPN используются в реальных инфраструктурах — более 30 тысяч поставленных продуктов и свыше 300 организаций-заказчиков. Причем речь идет как о государственных структурах, так и о коммерческом секторе. Этот опыт показывает, что решение масштабируется, устойчиво ведет себя в различных сценариях и соответствует требованиям регулятора не только формально, но и на практике.

### **Безопасность как управляемый процесс**

Современная криптографическая защита перестает быть отдельным инструментом и становится частью архитектуры ИТ-среды. На примере S-Crypto VPN хорошо видно, что эффективная система безопасности строится вокруг баланса нескольких факторов:

- соответствие нормативным требованиям;
- высокий уровень защиты каналов и данных;
- удобство для конечных пользователей;
- управляемость и снижение нагрузки на ИТ-службы.

Именно этот баланс сегодня определяет зрелость информационной безопасности — и становится ключевым фактором при выборе решений.