ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004:056 **DOI: 10.18413/2518-1092-2024-9-1-0-1**

Чайка Е.М.
Белов С.П.

ОБЗОР КРИПТОШЛЮЗОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

Белгородский университет кооперации, экономики и права,
ул. Садовая, д. 116а, г. Белгород, 308023, Россия

e-mail: desare48@yandex.ru, belovssergei@gmail.com

Аннотация
В данной статье рассматриваются решения отечественных производителей для организации защищенной корпоративной сети (криптошлюзы, VPN шлюзы), основные принципы работы данного оборудования, сценарии подключения и основные используемые протоколы, проведен анализ доступных для органов государственной и федеральной власти решений, согласно законодательства и требований регуляторов, проведен анализ стадий сертификации компонентов рассматриваемых решений, совместимость с отечественными операционными системами, рассматривается возможность применения комплексных решений в организациях.
Ключевые слова: шифрование; защищенные VPN-шлюзы; корпоративные сети; VipNet; Континент; Dionis
Для цитирования: Чайка Е. М., Белов С.П. Обзор криптошлюзов для защиты информации в корпоративных сетях // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 3-9. DOI: 10.18413/2518-1092-2024-9-1-0-1

Chayka E.M.
Belov S.P.

OVERVIEW OF CRYPTOGRAPHIC GATEWAYS FOR PROTECTION INFORMATION IN CORPORATE NETWORKS

Belgorod University of Cooperation, Economics and Law,
116a Sadovaya str., Belgorod, 308023, Russia

e-mail: desare48@yandex.ru, belovssergei@gmail.com

Abstract
This article discusses solutions from domestic manufacturers for the organization of a secure corporate network (cryptoslocks, VPN gateways), the basic principles of operation of this equipment, connection scenarios and the main protocols used, an analysis of solutions available to state and federal authorities, according to legislation and regulatory requirements, an analysis of the stages of certification of components of the solutions in question, compatibility with domestic ones The possibility of using integrated solutions in organizations is being considered.
Keywords: encryption; secure VPN gateways; corporate networks; ViPNet; Continent; Dionis
For citation: Chayka E.M., Belov S.P. Overview of cryptographic gateways for protection information in corporate networks // Research result. Information technologies. – T.9, №1, 2024. – P. 3-9. DOI: 10.18413/2518-1092-2024-9-1-0-1

ВВЕДЕНИЕ

Для осуществления эффективного менеджмента в современных реалиях, защита информации является обязательным условием и необходима на всех этапах развития деятельности организации. Информационная безопасность в организации основывается на комплексном подходе,

использовании как организационных мер, так и мероприятий по технической защите. В рамках данной статьи рассмотрим направление защиты информации непосредственно в корпоративных сетях и сетях Интернет (далее – сети). Но перед этим нужно остановится на основных задачах информационной безопасности. К ним относят: оперативный доступ к информационным услугам и к информации в целом в организации; актуальность и целостность информации, а также конфиденциальность данных.

Специалистами по информационной безопасности отмечается, что наиболее распространёнными угрозами в последнее время на сети организаций являются так называемые кибератаки, но при этом не стоит забывать про фишинг, вирусы и иное вредоносное ПО (программное обеспечение), высокий риск реализации угроз безопасности возможен и с использованием социальной инженерии.

Не стоит соответственно забывать и про технические ошибки, которые в свою очередь приводят к реализации уязвимостей в используемых информационных системах.

Для решения задач по защите сетей применяются такие методы как, внедрение межсетевых экранов, шифрование передаваемой информации, использование средства аутентификации и авторизации, системы регистрации событий безопасности и управление доступом к ресурсам.

Большая часть этого функционала реализована в программно-аппаратных комплексах для криптографической защиты трафика, передаваемого по каналам связи, при помощи так называемых «туннельных соединений» между компьютером пользователя и компьютером-сервером с использованием различных протоколов.

В состав данных комплексов опционально входят средства аутентификации и авторизации, с помощью которых происходит идентификация пользователей системы, определяются их права доступа к ресурсам; средства обнаружения и предотвращения вторжений (IDS/IPS) для обеспечения дополнительного уровня защиты.

Для реализации рассматриваемых «туннельных соединений» в организациях используется специализированное оборудование под названием VPN (Virtual Private Network) (криптографический шлюз, криптошлюз).

В последние годы отечественный рынок крипторешений стремительно активизировался, обосновать данную тенденцию можно несколькими причинами. Во-первых, активная политика регуляторов, нацеленная на защиту каналов связи, стимулирует организации обеспечивать безопасность передаваемых данных. Во-вторых, массовый переход на удаленную работу усилил потребность в реальной, а не только «бумажной» безопасности.

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ КРИПТОШЛЮЗОВ (СЦЕНАРИИ ПОДКЛЮЧЕНИЯ, ИСПОЛЬЗУЕМЫЕ ПРОТОКОЛЫ), КРИТЕРИИ ВЫБОРА

Для начала рассмотрим понятие VPN (виртуальная частная сеть) более подробно. Виртуальная частная сеть – это комплекс решений, обеспечивающих безопасную и качественную связь между территориально распределенными подсетями и группами пользователей через открытую сеть Интернет. Существуют два типичных сценария использования VPN: "site-to-site" (объединение площадок) и "client-to-site" (удаленный доступ).

Сценарий "site-to-site" – это безопасное соединение двух точек с помощью аппаратных шлюзов, которые обеспечивают высокую скорость соединения. Данные решения часто используются в глобальных сетях для подключения локальных сетей предприятий. Сценарии данного типа позволяют обеспечить шифрование всех пакетов данных при передаче через VPN туннель. Одним из преимуществ данного способа является масштабируемость, достаточно установить и настроить дополнительный VPN-шлюз для ввода в эксплуатацию нового удаленного офиса. При этом не стоит забывать о растущей потребности в создании более производительных каналов связи между центральными офисами организации, в некоторых случаях требуются каналы

с пропускной способностью более 100 ГБ, что требует использования кластера VPN-шлюзов. К рискам данного решения можно отнести уязвимости в аппаратном и программном обеспечении.

Рассмотрим другой сценарий реализации VPN "client-to-site". Он позволяет удаленным пользователям получить доступ к своим ресурсам во время работы из удаленного места, в этом способе реализации туннеля основные проблемой является с масштабируемость, при этом стоимость данного решения гораздо ниже, чем предыдущий рассматриваемый вариант.[10]

Дополнительным различием в построении шифрованных туннелей служит создание соединений используя на основе протокол L2 VPN (Layer 2 Virtual Private Network) и протокол L3 VPN (Layer 3 Virtual Private Network). Рассмотрим основные отличия данных способов создания виртуальных соединений. L2 VPN (VPN на основании канального уровня) – вид соединений работает на канальном уровне OSI.

Передача данных осуществляется при помощи фреймов, а не пакетов. Главным преимуществом этой технологии является виртуальное объединение удаленных локальных сетей в одну единую сеть [11].

При построении сетей VPN на основании L3 (Layer 3 Virtual Private Network) работа происходит на третьем уровне OSI (Open Systems Interconnection). L3 VPN создает сеть на основе IP-адресов, в которой удалённые устройства, так же, как и в L2VPN, обмениваются информацией независимо от расположения. Выбор технологии зависит от конкретных задач организации, если требуется объединить несколько сетей, которые будут работать как одна сетевая структура, то предпочтительно использовать L2 VPN, если нужно получить защищенную, гибкую в настройке систему то L3 VPN.

Современные шлюзы, рассматриваемые в рамках данной статьи, обеспечивает защиту, передаваемых по различным каналам связи как с использованием на канальном уровень OSI (L2 VPN), так и на сетевом уровне (L3 VPN).

VPN-шлюзы являются универсальными решениями, и обладают большим функционалом, при выборе важно основываться на многих параметрах, таких как наличие сертификатов регуляторов в сфере информационной безопасности, ценовая политика производителя оборудования, доступность технической поддержки, технические характеристики: пропускная способность оборудования, поддержка различных операционных систем, возможно запуска в среде виртуализации, дополнительные встроенные решения.

Нужно понимать, что выбор VPN-шлюза должен основываться на анализе требований конкретной организации, а также на обеспечении безопасности и удобства использования для конечных пользователей.

ОБЗОР РЕШЕНИЙ, ПРЕДСТАВЛЕННЫХ НА ОТЕЧЕСТВЕННОМ РЫНКЕ.

По данным интернет-издания www.anti-malware.ru в 2023 год на Российском рынке представлены продукты следующих российских вендоров:

- «Атликс-VPN» («НТЦ Атлас»);
- «ЗАСТАВА» («ЭЛВИС-ПЛЮС»);
- «Континент» («Код Безопасности»);
- «С-Терра Шлюз» («С-Терра СиЭсПи»);
- «ФПСУ-IP» («АМИКОН», «ИнфоКрипт»);
- ALTELL NEO («АльтЭль»);
- Diamond VPN (ТСС);
- Dionis-DPS («Фактор-ТС»);
- NGate («КриптоПро»);
- ViPNet Coordinator HW («ИнфоТеКС»).[7]

Рассмотрим три популярных продукта, применяемых в государственных и федеральных органах Российской Федерации. Технические характеристики были получены с официальных ресурсов производителей рассматриваемого оборудования.

Dionis DPS, производство компании ООО «Фактор-ТС». Это единый центр управления защитой сети, сертифицированный ФСБ и ФСТЭК России. Применяется для защищенной передачи конфиденциальной информации через сети общего пользования в качестве пограничного устройства между защищаемыми локальными сетями и транспортной средой. В ПАК (программно-аппаратный комплекс) Dionis DPS реализованы алгоритмы шифрования в соответствии с государственными стандартами Российской Федерации. Комплекс поддерживает два варианта VPN-туннелей, основное отличие которых состоит в том, что при их построении используются две разные схемы распределения ключей шифрования (симметричная и несимметричная). Программные компоненты комплекса включают в себя «DiSec» (клиент для обеспечения защищенного доступа мобильных абонентов), «DioPost» (защищенный почтовый клиент).

Модельный ряд ориентирован как на небольшие компании, так и на крупные организации с большими центрами обработки данных. Обеспечивается скорость шифрования от 100 Мбит/с до 8000 Мбит/с. Имеется сертификат ФСТЭК России на МЭ типа «А» 2-го класса защиты и на СОВ уровня сети 2-го класса защиты, сертификат ФСБ России для СКЗИ (средства криптографической защиты информации) по классам КС1, КС3 [6].

VipNet Coordinator HW/VA, производство компании АО «ИнфоТеКС».

ПАК VipNet Coordinator HW - ряд криптошлюзов (криптомаршрутизаторов) предназначенных для построения виртуальной сети VipNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика.

Благодаря функциям криптографической защиты данных, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК VipNet Coordinator HW является оптимальным средством защиты компьютерных сетей организаций от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи. Программный комплект состоит из ViPNet Administrator 4 (программное обеспечение, предназначенное для развертывания и администрирования сети ViPNet корпоративного масштаба), ViPNet Client 4U (программный комплекс ViPNet Client 4U для защиты рабочих мест пользователей и мобильных устройств), ViPNet Деловая почта (программное обеспечение для обмена электронными письмами в защищенной сети ViPNet).

В зависимости от модификации ПАК VipNet Coordinator HW позволяет организовать защищенный доступ как в ЦОДы (центры обработки данных), так и в корпоративную облачную инфраструктуру, может быть использован для защиты филиалов организаций, небольших удаленных офисов, удаленных рабочих мест, а также терминалов и устройств, в том числе обеспечивая безопасное подключение к корпоративной защищенной сети по беспроводным каналам связи. Модельный ряд включает в себя оборудование с широким диапазоном производительности: от 75 Мбит/с до 10 000 Мбит/с. Имеются сертификаты соответствия по требованиям безопасности ФСБ России и ФСТЭК России. Из особенностей также доступно виртуализированное исполнение – VipNet Coordinator VA (СКЗИ класса КС1) для развёртывания на популярных платформах виртуализации [9].

АПКШ «Континент», производство компании ООО «Код Безопасности». Представляет собой централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ. Модельный ряд позволяет подобрать решение для организации связи с удалёнными подразделениями, филиалами или партнёрами по каналам связи с различной пропускной способностью и возможностью централизованного управления. Производительность L2 VPN варьируется от 120 Мбит/с до 40 000 Мбит/с. При этом на специализированной аппаратной платформе «Континент 3.9 IPC-3000FC-40G» реализован криптоускоритель с производительностью VPN ГОСТ до 40 Гбит/с и задержками обработки трафика около 50 мкс. В наличии сертификаты соответствия по требованиям безопасности ФСТЭК России, ФСБ России, Минкомсвязи и Минобороны России. Программные средства, включенные в комплекс: Континент-АП (для

организации доступа удаленных пользователей по защищенному каналу к ресурсам, защищаемым средствами АПКШ).[8]

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА КРИПТОШЛЮЗОВ

Систематизируем основные характеристики трех рассматриваемых решений, представленных в этой статье:

Согласно требованиям регуляторов ФСБ и ФСТЭК в информационных системах персональных данных, государственных информационных системах, автоматизированных системах управления производственными и технологическими процессами применяются только сертифицированные средства защиты информации. Информация о сертификации криптошлюзов (Таблица 1) и программных компонентов (Таблица 2) представлены ниже [1-5].

Таблица 1

Сертификация криптошлюзов

Table 1

Certification of cryptographic gateways

Наименование решения	Сертификат ФСБ КС1/КС2/КС3	Сертификат ФСТЭК
Дионис DPS/NX	+/-/+	+
Vipnet Coordinator	+/+/+	+
Континент АПКШ	+/+/+	+

Таблица 2

Сертификация программных компонентов

Table 2

Certification of software components

Наименование ПО	Сертификат ФСБ Windows	Сертификат ФСБ Linux	Сертификат ФСТЭК Windows	Сертификат ФСТЭК Linux
Dionis DiSec	+	-	+	-
Dionis DioPost	+	-	+	-
ViPNet Administrator 4	+	-	+	-
ViPNet Client 4U	+	-	+	-
ViPNet Деловая почта	+	-	+	-
Континент-АП	+	+	+	+

Рассматривая результаты сравнения наличия сертификатов видно, что большинство продукции не имеет действующих сертификатов соответствия (многие продукты в настоящий момент проходят сертификацию), следовательно, в одиночном исполнении криптошлюзы (VPN-шлюзы) полностью подходят по требования законодательства, а вот использование прикладного программного обеспечения в органах государственной

и федеральной власти попадает под сомнение. Решение данной проблемы только в одном, это ожидание завершения процедур тестирования и сертификации программного обеспечения.

И все же, представленные комплексные решения получили высокие положительные оценки среди специалистов информационной безопасности на рынке криптомашрутизаторов и VPN-шлюзов.

В настоящее время Vipnet Coordinator применяется в государственных структурах для обеспечения безопасности при построении сети, Dionis DPS широкое применение получил в федеральных органах, Континент-АП – в реализациях государственных информационных систем федерального уровня.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели в данной статье определенный класс устройств, используемые в качестве криптомаршрутизаторов и VPN-шлюзов. Из технических характеристик наблюдается, что рассматриваемые решения выполняют не одну, изначально заложенную, функцию, а являются более универсальными средствами для обеспечения безопасности и конфиденциальности информации при передаче по сети. В функционал, помимо создания шифрованных виртуальных туннелей, входят дополнительные сервисы: DHCP, DNS, Proxy-серверы.

Какое дальнейшее развитие этого класса ждет нас в будущем? Либо это будет «комбайн» функций, либо развитие пойдет по дроблению на отдельные устройства и сервисы, пока ответить однозначно сложно. При этом развитие технологий идет по пути использования универсальных устройств, такой подход позволяет строить систему безопасности из однородных компонентов, что положительно сказывается на возможностях администрирования и обслуживания сетей. Также к преимуществам универсальности подобных устройств можно отнести экономическую выгоду и удобство для организаций.

На отечественном рынке криптошлюзов с каждым годом появляются новые игроки, большую роль в этом развитии имеют регуляторы в области информационной безопасности. Нормативные акты ФСБ и ФСТЭК положительно влияют на развитие рынка отечественных сертифицированных VPN решений. Это позволяет российским производителям участвовать в постепенной замене импортных решений и помогает развивать отечественные аналоги. Но при этом одной из ключевых проблем для рынка криптошлюзов в России остается отсутствие аппаратных платформ для построения полностью импортонезависимого продукта.

Список литературы

1. ФЗ №149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».

2. Постановление правительства №1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Приказ №17 ФСТЭК от 11.02.2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Приказ №21 ФСТЭК от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Приказ №31 ФСТЭК от 14.03.2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

6. Возможности Dionis DPS. URL: https://dps.factor-ts.ru/vozmozhnosti, дата обращения: 01.12.2023 [Электронный ресурс].

7. Зензин И. «Обзор криптографических шлюзов российских и зарубежных производителей». URL: https://www.anti-malware.ru/analytics/Market_Analysis/cryptographic-gateways-russian-and-foreign-manufacturers-2017, дата обращения: 01.12.2023 [Электронный ресурс].

8. Комплекс безопасности Континент Версия 4 Руководство администратора Принципы функционирования URL: https://www.securitycode.ru/upload/iblock/a6c/mjqueclwoehg014tilmlinzmbwxfdlc5/Continent-Basics-AdminGuide.pdf, дата обращения: 01.12.2023 [Электронный ресурс].

9. Криптографический шлюз безопасности – Межсетевой экран нового поколения VipNet Coordinator HW 5. URL: https://infotecs.ru/products/vipnet-coordinator-hw-5/, дата обращения: 01.12.2023 [Электронный ресурс].

10. Сарычев Д. «Как выбрать корпоративный VPN-шлюз», URL: https://www.anti-malware.ru/practice/methods/How-to-choose-VPN-gateway#part4, дата обращения: 01.12.2023 [Электронный ресурс].

11. SIM-Networks, Каналы связи L2 и L3 VPN – отличия физических и виртуальных каналов разного уровня. URL: https://www.sim-networks.com/ru/blog/the-difference-between-layer-2-and-layer-3-networks, дата обращения: 01.12.2023 [Электронный ресурс].

References

1. Federal Law No. 149 dated 07/27/2006 "On Information, Information Technologies and Information Protection".

2. Government Resolution No. 1119 dated 11/01/2012 "On approval of requirements for the protection of personal data during their processing in personal data information systems".

3. Order No. 17 of the Federal Customs Service of 11.02.2013 "On approval of requirements for the protection of information that does not constitute a State Secret contained in State information systems."

4. FSTEC Order No. 21 dated 02/18/2013 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems".

5. FSTEC Order No. 31 dated 03/14/2014 "On Approval of Requirements for Ensuring Information Protection in Automated Control Systems for Production and Technological Processes at Critical Facilities, potentially Dangerous facilities, as well as facilities that pose an increased danger to human life and health and to the environment".

6. Features of Dionis DPS Source: https://dps.factor-ts.ru/vozmozhnosti, date of access: 12/01/2023, electronic text.

7. Zenzin I. "Overview of cryptographic gateways of Russian and foreign manufacturers" Source: https://www.anti-malware.ru/analytics/Market_Analysis/cryptographic-gateways-russian-and-foreign-manufacturers-2017, accessed: 12/01/2023, electronic text.

8. Security Complex Continent Version 4 Administrator's Guide Principles of operation https://www.securitycode.ru/upload/iblock/a6c/mjqueclwoehg014tilmlinzmbwxfdlc5/Continent-Basics-AdminGuide.pdf, accessed: 12/01/2023, electronic text

9. Cryptographic Security Gateway – A new generation Firewall ViPNet Coordinator HW 5 Source: https://infotecs.ru/products/vipnet-coordinator-hw-5 /, date of access: 12/01/2023, electronic text.

10. Sarychev D. "How to choose a corporate VPN gateway", Source: https://www.anti-malware.ru/practice/methods/How-to-choose-VPN-gateway#part4, date of access: 12/01/2023, electronic text.

11. SIM Networks, L2 and L3 VPN communication channels – differences between physical and virtual channels of different levels. Source: https://www.sim-networks.com/ru/blog/the-difference-between-layer-2-and-layer-3-networks, date of access: 12/01/2023, electronic text.

Чайка Евгений Михайлович, магистрант 2 курса кафедры информационная безопасность
Белов Сергей Павлович, доктор технических наук, профессор, профессор кафедры информационной безопасности

Chayka Evgeny Mikhailovich, 2nd year Master's student, Department of Information Security
Sergey Pavlovich Belov, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security