Лапшин И.О.,

кандидат технических наук, доцент
Московский университет МВД России имени В.Я. Кикотя

Стручков И.С.

Московский университет МВД России имени В.Я. Кикотя

Броненкова Ю.В.

Академия управления МВД России (г. Москва)

Управление кибербезопасностью на основе технологии виртуальных сетей

При анализе кибербезопасности распределенных информационных сетей следует учитывать не только угрозы со стороны внешних злоумышленников, но и потенциальные риски, исходящие от внутренней сети, доступ к которой зачастую бывает более уязвим для нарушений.

При этом важно создать такую интегрированную защищенную среду в телекоммуникационной инфраструктуре, чтобы обеспечить надежную безопасность коммуникаций, технических средств и информационных ресурсов. Это требует учета взаимодействия с внешними техническими средствами и ресурсами, способствуя формированию эффективной защиты от возможных угроз.

Задачи защиты сетевой структуры.

С учетом актуальных требований, касающихся киберзащиты сетевой инфраструктуры и передачи сетевого трафика, возникает необходимость в решении следующих задач:

– подготовка нужного количества квалифицированных специалистов в области кибербезопасности;

– нормативно-правовое регулирование защищенного сетевого взаимодействия, в том числе между ведомствами;

– оперативное реагирование на появление новых угроз кибербезопасности, что требует ее постоянного мониторинга и анализа;

– расширение и совершенствование инструментов комплексной защиты от угроз в области кибербезопасности;

– оптимизация расходов на систему защиты информации при учете перспективности применяемых подходов и технологий.

Новые решения.

Одним из элементов системы киберзащиты является аппаратно-программный комплекс шифрования (АПКШ) «Континент» для создания магистральных VPN-сетей повышенного уровня безопасности с использованием алгоритмов шифрования государственного стандарта[1].

[1] Информация о продуктах компании «Код Безопасности». URL: http://www.securitycode.ru/products/ (дата обращения: 29.11.2024).

Комплекс направлен на применение в трех направлениях:

– использование межсетевых экранов для защиты внутренних сетевых сегментов от несанкционированного доступа;

– осуществление криптографической защиты (согласно ГОСТ 28147–89) передаваемых данных;

– построение информационных подсистем с разграничением физического доступа.

Если говорить более детально, то областями применения «Континента» выступают:

– защита от вредоносного воздействия внешнего периметра сети со стороны сетей общего пользования;

– создание между территориально распределенными сетями отказоустойчивой VPN-сети;

– обеспечение защиты сетевого трафика в мультисервисных сетях (VoIP, Video Conference);

– разделение на сегменты сети с различным уровнем доступа;

– организация мобильного защищенного удаленного доступа к сети;

– защита трафика для пользователей, использующих беспроводную сеть;

– организация между конфиденциальными сетями защищенного межсетевого взаимодействия.

АПКШ «Континент» объединяет межсетевой экран и средство построения виртуальных частных сетей, обеспечивает защиту информационных сетей организации от вторжения со стороны сетей передачи данных, конфиденциальность при передаче информации по открытым каналам связи, безопасный доступ пользователей VPN к ресурсам сетей общего пользования, а также защищенное взаимодействие сетей различных организаций. Является продуктом, сертифицированным ФСТЭК и ФСБ. Является одной из немногих российских сертифицированных программ с высокой производительностью (в режиме VPN – 800 Мбит/сек).

«Континент» широко используется государственными структурами России, например Казначейством Российской Федерации.

Подчеркнем, что среди отечественных VPN-решений «Континент» выделяется:

– централизованным управлением компонентами комплекса, включая дистанционное обновление программного обеспечения;

– работой в необслуживаемом режиме, не требуя специального персонала;

– возможностью обработки высокоприоритетного трафика с защитой голосовой информации (VoIP) и видеоконференций в гетерогенных сетях;

– резервированием гарантированной полосы пропускания, позволяющим прохождение электронной почты даже при активном использовании IP-телефонии;

– поддержкой работы через Dial-Up и ADSL-соединения, а также спутниковые каналы связи;

– поддержкой протоколов динамической маршрутизации и технологии VLAN;

– взаимодействием с системами управления сетью, что позволяет постоянно контролировать состояние комплекса;

– высокой надежностью и отказоустойчивостью, обеспечиваемой за счет криптошлюза на серверах, предназначенных для использования в жестких эксплуатационных условиях;

– возможностью «горячего» резервирования криптошлюзов для построения сетей с высокой доступностью;

– простотой внедрения, характеризующейся тем, что при любой конфигурации защищаемой сети «Континент» может быть установлен без внесения изменений в существующие технологии взаимодействия с открытыми сетями (Internet).

Технологии ViPNet[1] включены в Единый реестр российского программного обеспечения, полностью соответствуя требованиям государственной программы импортозамещения.

Комплекс включает три основных компонента:

– координатор – программно-аппаратный комплекс, формируемый из специального оборудования и поддерживающий маршрутизацию пакетов между участниками обмена; обеспечивающий регистрацию и предоставление информации о текущих IP-адресах и способах подключения объектов сети; поддерживающий работу защищенных компьютеров сети в VPN от имени одного адреса и работу защищенных компьютеров локальной сети, а также тунелирование пакетов в защищенное соединение от заданных адресов незащищенных компьютеров; организующий безопасное подключение части

[1] Подр.: Гусев В.В., Чаплыгин В.Е. Администрирование системы защиты информации ViPNet (Windows & Linux). М.: Горячая линия – Телеком, 2018. 366 с.; Прудников А.И., Шахов В.Г. Особенности использования технологии ViPNet для защиты информации в корпоративных сетях. URL: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniyatehnologii-ViPNet-dlya-zaschity-informatsii-v-korporativnyh-setyah. (дата обращения: 29.11.2024); Акинина Л.Н., Попов В.Б., Перехрест Р.Д. Программно-аппаратные комплексы ViPNet и их использование в корпоративных сетях // Научный вестник Крыма. 2016. № 3. URL: https://cyberleninka.ru/article/n/ programmno-apparatnye-kompleksy-ViPNet-i-ih-ispolzovanie-v-korporativnyh-setyah (дата обращения: 29.11.2024); Лапшин И.О., Мамлеев Р.Р. Администрирование системы защиты информации ViPNet : учебно-методическое пособие. М.: МосУ МВД России им. В. Я. Кикотя, 2024. 169 с.

компьютеров локальной сети к Интернету без их физического отключения от локальной сети организации;

– администратор – как центр управления сетью, который обеспечивает централизованное управление сетью и формирует структуру VPN и управляет логику ее работы; осуществляет централизованное обновление программного обеспечения и функционала компонентов VPN; производит мониторинг событий VPN; удаленно управляет ресурсами VPN; выполняет функции удостоверяющего центра для участников VPN;

– клиент – программный модуль, позволяющий защитить компьютер от попыток несанкционированного доступа как из глобальной, так и из локальной сети, управляющий терминалом, где установлен модуль, а также осуществляющий фильтрацию трафика по уровню сервиса и протокола. С его помощью контролируются активность приложений и блокировка нежелательных приложений без участия пользователя.

Таким образом, ViPNet представляет комплексное решение, включающее разнообразные программные продукты и сетевые технологии для эффективного управления кибербезопасностью. Обеспечивает защиту рабочих станций от внешних и внутрисетевых угроз путем фильтрации трафика, а также безопасную работу удаленных сотрудников в корпоративных системах и сервисах.

Технологические решения на базе программных комплексов «Континент» и ViPNet, удовлетворяя современным практическим потребностям, обеспечивают надежную защиту данных, соответствуя высоким требованиям кибербезопасности. Этот процесс включает в себя комплекс мероприятий, направленных на постоянный мониторинг и оперативное внедрение усовершенствований в области кибербезопасности.

Королев А.С.

Ленинградский областной филиал
Санкт-Петербургского университета МВД России (п. Мурино)

Анализ психологических факторов, способствующих вовлечению молодежи в экстремизм через социальные сети

В современном мире проблема распространения экстремизма в молодежной среде через Интернет и социальные сети приобретает все большую остроту. Значительная часть экстремистских преступлений совершается молодыми людьми, завербованными онлайн. Интернет предоставляет экстремистам широкие возможности для пропаганды своих идей, вербовки новых сторонников и координации деятельности. Целью данной статьи является анализ