МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2025.153.44

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОЙ КОРПОРАТИВНОЙ СЕТИ С ПРИМЕНЕНИЕМ VPN

Научная статья

Перухин М.Ю.[1,] *, Воронина Л.Т.[2], Сафиуллина Л.Х.[3], Алексеева А.А.[4]

[1, 2, 3, 4] Казанский национальный исследовательский технологический университет, Казань, Российская Федерация

* Корреспондирующий автор (perukhin[at]inbox.ru)

Аннотация

В статье рассматриваются возможные способы защиты корпоративной информации. Целью является проектирование защищенной корпоративной сети с применением VPN. Рассмотрена методика проектирования защищенной корпоративной сети (КС) с удаленными филиалами. Авторы предлагают рекомендации для обеспечения устойчивой связи с корпоративной сетью в головном офисе и филиалах. Для большей безопасности предлагается использовать принцип нулевого доверия, при котором каждый пользователь при обращении к ресурсам будет проходить двухфакторную аутентификацию. При этом важно грамотно настроить политику безопасности во избежание потери доступа сотрудников в корпоративную сеть. В работе представлены методология построения безопасной КС, в которой используются такие этапы как изучение структуры КС и выбор технологий для связи головной организации и филиалов, реализация КС с учётом прав доступа, определение расположения серверов, коммутационных шкафов и телекоммуникационных розеток, создание логической структуры сети, подбор активного сетевого оборудования, распределение сетевых адресов и подсетей, создание физической структуры сети и разработка политик безопасности, списков доступа и сценариев их реализации.

Ключевые слова: корпоративная сеть, защита информации, локальная сеть, политика безопасности, защищенность.

DESIGNING A SECURE CORPORATE NETWORK WITH VPN APPLICATION

Research article

Perukhin M.Y.[1,] *, Voronina L.T.[2], Safiullina L.K.[3], Alekseeva A.[4]

[1, 2, 3, 4] Kazan National Research Technological University, Kazan, Russian Federation

* Corresponding author (perukhin[at]inbox.ru)

Abstract

The article examines possible ways to protect corporate information. The aim is to design a secure corporate network using VPN. The methodology of designing a secure corporate network (CN) with remote branches is discussed. The authors offer recommendations to ensure stable communication with the corporate network in the head office and branches. For greater security, it is proposed to use the principle of zero trust, in which each user will undergo two-factor authentication when accessing resources. At the same time, it is important to properly configure the security policy to avoid the loss of access of employees to the corporate network. The paper presents a methodology for building a secure CN, which uses such stages as the study of the structure of the CN and the choice of technologies for communication of the parent organisation and branches, implementation of the CN taking into account access rights, determining the location of servers, switching cabinets and telecommunication outlets, creating a logical network structure, selection of active network equipment, distribution of network addresses and subnets, creation of the physical network structure and development of security policies, access lists and scenarios for their implementation.

Keywords: corporate network, information protection, local network, security policy, security protection.

Введение

Сегодня эффективное функционирование предприятий невозможно представить без использования современных информационных технологий. Организации не ограничены территориально одним местом и активно внедряют сетевые технологии для дистанционного взаимодействия с партнерами, а также предоставляют сотрудникам возможность удаленной работы. Эти меры способствуют повышению гибкости бизнес-процессов и обеспечивают эффективное распределение ресурсов, при этом создавая дополнительные вызовы в области информационной безопасности [1].

По данным авторитетной компании, специализирующейся на информационной безопасности в корпоративном секторе InfoWatch, в 2023-ем году в Интернет утекло 1,12 миллиарда записей персональных данных, что на 60% больше по сравнению с 2022-ым годом, когда было скомпрометировано около 700 миллионов записей. Несмотря на то, что количество инцидентов утечек сократилось на 15% и составило 656 случаев, средний объем данных, украденных за один инцидент, удвоился – с 0,9 миллиона до 1,7 миллиона записей. Из российских компаний утекло 95 крупных баз данных, что на 28% больше, чем в 2022-ом году. Более 80% утечек было связано с кибератаками, и 35% компаний считают утечки персональных данных одной из самых актуальных угроз [2], [3].

В сложившейся ситуации корпоративная информация, передаваемая в онлайн-среде, подвержена риску перехвата и несанкционированного использования злоумышленниками. Под угрозой оказываются не только конфиденциальные данные, содержащиеся в важных документах, но и учетные данные для доступа к корпоративным системам, включая

электронную почту, системы электронного документооборота, дампы внутренних баз данных и другие критически важные сервисы [4]. Обеспечение безопасности данных при их передаче в корпоративных сетях (КС) является серьезной и актуальной задачей. Несмотря на широкое разнообразие существующих методов защиты КС, крайне важно постоянно внедрять новые подходы к кибербезопасности, поскольку злоумышленники непрерывно совершенствуют свои инструменты и находят способы обхода действующих защитных механизмов [5]. Только проактивное обновление и адаптация мер безопасности позволяют противостоять новым угрозам и минимизировать риски утечек данных и компрометации систем.

Одним из способов организации распределенных защищенных информационных систем (ИС) является применение протоколов VPN (Virtual Private Network), которые обеспечивают создание виртуальных туннелей связи через сеть Интернет [6]. В настоящей статье будет рассмотрена методика проектирования защищенной корпоративной сети (КС) с удаленными филиалами.

Предлагаемая методика будет состоять из следующих этапов:

- изучение структуры КС и подбор технологии и оборудования для объединения головной организации и ее филиалов в КС;
- реализация КС с учетом различных прав доступа;
- определение места расположения серверного оборудования и коммутационных шкафов, а также телекоммуникационных розеток;
- создание логической структуры сети организации;
- подбор активного сетевого оборудования;
- разработка политик безопасности, списков доступа к ресурсам сети и сценариев реализации политики безопасности.

Далее мы рассмотрим технологии VPN и рассмотри процесс разработки защищенной КС на их базе.

1.1. Общие принципы обеспечения безопасности сети на базе технологии VPN

Для защиты КС [7] разработаны способы и методики, которые широко применяются на всей территории РФ.

Прежде чем переходить к разработке системы защиты, необходимо провести аналитические работы по оценке защищённости. Они могут проводиться по нескольким направлениям:

1) комплексный анализ информационных систем;

2) разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-алгоритмическому обеспечению работы информационных систем (ИС) компании [8];

3) организационно-технологический анализ ИС компании;

4) экспертиза решений и проектов;

5) работы по анализу документооборота;

Корпоративная сеть должна быть способна обеспечить единую базу данных для всех организаций, предоставлять надёжную телефонную и факсимильную связь вне зависимости от расстояния. Обобщенно КС можно представить согласно рис.1.

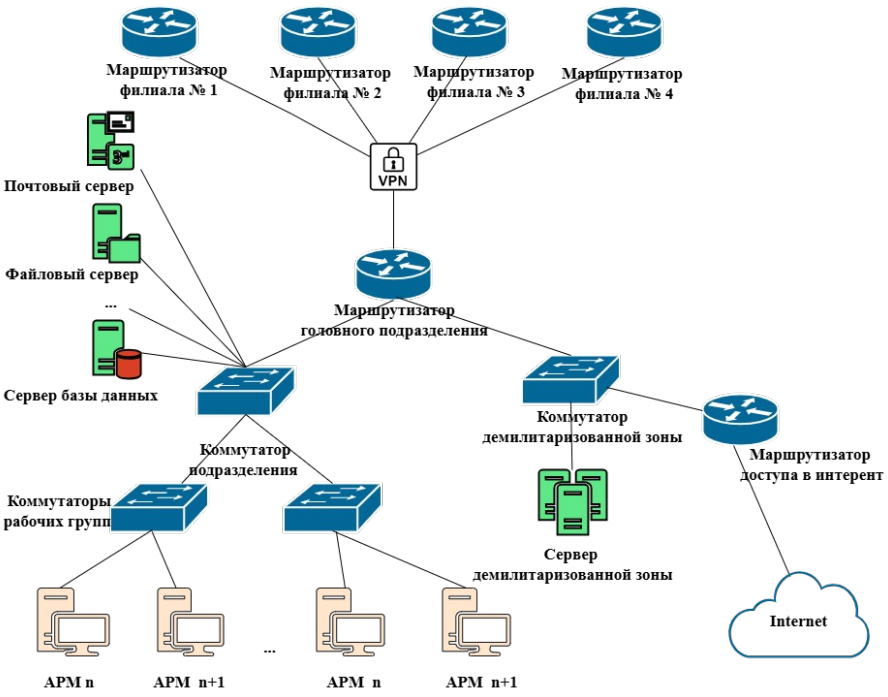

Рисунок 1 - Схема обобщённой корпоративной сети

DOI: https://doi.org/10.60797/IRJ.2025.153.44.1

Виртуальная частная сеть (Virtual Private Network – VPN) появилась как альтернатива, которая позволяет защищать связь между удаленными работниками и серверами организации, независимо от того, где находятся работники. В [9] VPN описывают как традиционный подход для сквозного безопасного соединения между двумя конечными точками с использованием публичной или общей телекоммуникационной инфраструктуры, где конфиденциальность обеспечивается с помощью протокола туннелирования и шифрования. Существует четыре типа архитектуры защиты информации с использованием технологии VPN [10]:

1) *VPN локальной сети* (Local Area Network VPN), которая обеспечивает защиту данных внутри корпоративной сети от несанкционированного доступа. Она включает протоколы шифрования конфиденциальных данных, контроль доступа, защиту паролей и регистрацию коллизий, а также безопасность операционных систем.

2) *Внутрикорпоративная VPN* (Intranet VPN), которая ответственна за безопасные соединения между подразделениями распределенной компании, так же как VPN локальной сети использует шифрование, поддерживает критически важные транзакционные приложения и сервисы (СУБД, почта, FTP).

3) *VPN с удаленным доступом* обеспечивает безопасное подключение удаленных сотрудников и подразделений через открытые сети. Включает надежную идентификацию и аутентификацию, а также управление защитными ресурсами распределенной системы.

4) *Межкорпоративная VPN* предоставляет безопасные соединения с внешними организациями, клиентами и партнерами, позволяя обмениваться конфиденциальной информацией без риска утечек. Поддерживает аутентификацию и контроль доступа к ресурсам.

Рассмотренные архитектуры VPN реализуются в программно-аппаратных комплексах, обеспечивающих криптографическую защиту передаваемого трафика с использованием туннельных соединений между устройствами пользователя и серверами. Эти комплексы поддерживают различные протоколы шифрования, а также могут включать средства аутентификации и авторизации, которые отвечают за идентификацию пользователей и управление их правами доступа. Дополнительно могут применяться системы обнаружения и предотвращения вторжений (IDS/IPS), что создает дополнительный уровень защиты. В рамках организации для этих целей используется специализированное оборудование, такое как криптографические шлюзы (VPN) [11].

Туннельная схема организации КС представлена на рис.2.

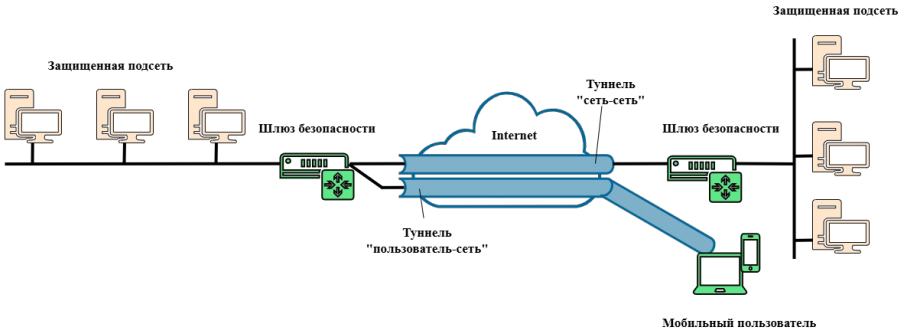

Рисунок 2 - Туннельная схема организации VPN сети
DOI: https://doi.org/10.60797/IRJ.2025.153.44.2

Для создания туннелей в VPN используются два основных метода:

- инкапсуляция пакетов с шифрованием в рамках одного протокола;
- создание виртуального IP-туннеля между узлами сети с использованием технологии туннелирования.

Эти туннели защищают передаваемую информацию от перехвата и анализа злоумышленниками. Основные элементы архитектуры VPN включают VPN-сервер, алгоритмы шифрования, систему аутентификации и протоколы связи. Выбор этих компонентов напрямую влияет на безопасность, производительность и совместимость сети, что делает их ключевыми аспектами при проектировании VPN для организаций. Такой же принцип можно использовать и для организации автоматизированного рабочего места (АРМ) сотрудника, работающего удаленно.

Основное свойство технологии туннелирования заключается в возможности не только зашифровать поле данных, но и весь исходный пакет, включая заголовки. Это важно, потому что злоумышленник может попытаться получить информацию о внутренней структуре КС из заголовка исходного пакета (например, количество хостов и сегментов КС, их IP-адреса) [12]. Зашифрованный пакет инкапсулируется в другой пакет с открытым заголовком, который передается по соответствующему туннелю (рис.3). Когда конечная точка туннеля достигается, внешний пакет деинкапсулируется из внутреннего пакета, дешифруется, и его заголовок используется для передачи по внутренней сети или подключенному к локальной сети мобильному пользователю [10]. Схема пакет с инкапсулируемым заголовком представлена на рис.4.

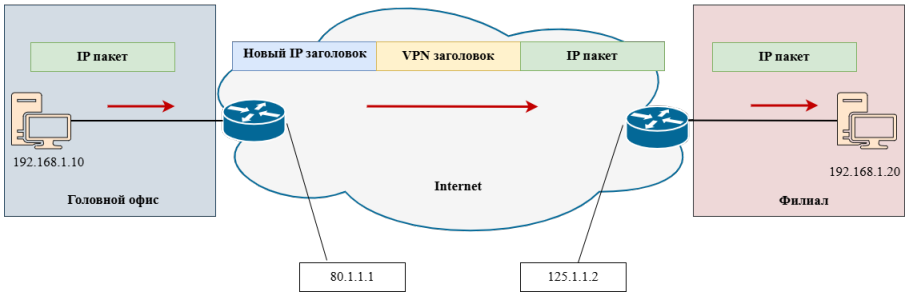

Рисунок 3 - Схема туннелирования пакетов в технологии VPN
DOI: https://doi.org/10.60797/IRJ.2025.153.44.3

Адрес отправителя 80.1.1.1	Адрес получателя 125.1.1.2	VPN заголовок	Адрес отправителя 192.168.1.10	Адрес получателя 192.168.1.20	Данные

Рисунок 4 - Инкапсулируемый пакет
DOI: https://doi.org/10.60797/IRJ.2025.153.44.4

Виды протоколов и соединений VPN

В настоящий момент существует следующий набор стандартных протоколов для VPN [5]:

- GRE;
- L2TP/IPsec;
- IKEv2/IPSec;
- IPSec;
- OpenVPN/ TCP;
- Easy Cisco VPN;
- Веб-VPN;
- L2/L3 VPN
- PPTP и др.

На их описании не будем останавливаться, поскольку в [5] все они рассмотрены достаточно подробно. Важно отметить, что для различных соединений различные протоколы. Так, например, для Remote Access VPN (на основе удаленного доступа) используется SSL/TLS, а для Site-to-Site VPN, который объединяет несколько офисов одной компании в единую корпоративную сеть с защищенными каналами между сетями используется IPsec. Используемые для построения КС протоколы VPN должны обладать надежным алгоритмом шифрования.

Соединение VPN может осуществляться:

-централизованно – через центральный VPN-сервер;

-децентрализованно.

2.1. Реализация КС с учетом различных прав доступа

Конфигурация VPN, которая включает протоколы VPN, алгоритмы шифрования, методы аутентификации и протоколы туннелирования, имеют решающее значение для управления безопасностью сети. При этом использовать VPN технологии для реализации безопасной КС необходимо с учетом прав доступа для обеспечения полноценной защиты. Рекомендации для проектирования КС в таком случае будут следующие:

- сегментация сети: VPN позволяет создавать виртуальные подсети, к которым будет доступ только у ограниченного круга пользователей;

- дополнительные требования для привилегированных пользователей: установка PAM (Privileged Access Management) решений, которые позволяют после подключения по VPN предоставлять доступ только к серверу PAM, а от него уже осуществлять доступ ко всем остальным системам;

- мониторинг, журналирование и аудит событий: использование VPN-решения интегрированной системой мониторинга и логирования позволят оперативно реагировать на аномальные попытки доступа и нарушения;

- использование VPN с динамическим распределением прав: для более высокой гибкости VPN-решения могут поддерживать динамическое управление правами.

Для большей безопасности предлагается использовать принцип нулевого доверия, при котором каждый пользователь при обращении к ресурсам будет проходить двухфакторную аутентификацию. При этом важно грамотно настроить политику безопасности во избежание потери доступа сотрудников в корпоративную сеть.

2.2. Определение места расположения оборудования

При выборе программного обеспечения VPN для безопасной настройки КС помимо вышеприведённых рекомендаций необходимо учитывать, количество, качество и размещение оборудования в соответствии со структурой предприятия. Серверные располагаются в каждом филиале, совместно с активным оборудованием. В центральном офисе как правило располагаются головной сервер, почтовый сервер, DNS-сервер, веб-сервер, DHCP-сервер, файловый сервер, сервер резервного копирования и другие корпоративные серверы, на которые устанавливаются системы контроля. К таким системам контроля могут быть отнесены SIEM, DAM и DCAP решения. Помимо этого, в

серверных необходимо предусмотреть наличие средств бесперебойного питания, ограничения физического доступа. Для обеспечения наилучшей защиты конфиденциальной информации рекомендуется отказаться от сторонних систем хранения данных и виртуальных машин, а также от облачных сервисов [13].

2.3. Создание логической структуры сети организации

Для усиления защиты целесообразно внедрить сетевую сегментацию, которая позволит на основе одной физической сети создать несколько изолированных логических сегментов. Это можно реализовать посредством виртуальных локальных сетей (VLAN), разделяющих инфраструктуру на группы с различными уровнями доступа и ограничениями. Такое разделение снижает риски несанкционированного доступа и локализует потенциальные угрозы, препятствуя их распространению по всей сети [14].

Для обеспечения доступа локальной сети к Интернету применяется технология трансляции сетевых адресов NAT (Network Address Translation), скрывающая внутренние IP-адреса от внешней сети и повышающая безопасность и конфиденциальность данных. Использование NAT также необходимо, поскольку интернет-маршрутизаторы не поддерживают внутренние (зарезервированные) адреса.

Для обеспечения устойчивой связи с корпоративной сетью в головном офисе и филиалах рекомендуется иметь минимум два альтернативных интернет-канала. Если имеются сотрудники, работающие удаленно, которые могут подключаться через разнообразных провайдеров, необходимо предусмотреть универсальный резервный канал. В случае использования домашнего интернета как рабочего средства рекомендуется назначить сотруднику статический IP-адрес и ограничить доступ к корпоративной сети и облачным ресурсам компании исключительно с этого адреса для повышения безопасности и контроля местоположения.

2.4. Подбор сетевого оборудования

Для стабильного и безопасного соединения необходимо правильно подобрать активное коммуникационное оборудование. На мировом рынке существует множество компаний, производящих различное сетевое оборудование (коммутаторы, межсетевые экраны, маршрутизаторы и т.п.), однако с 2025 года организации будут ограничены в выборе средств защиты информации. В соответствии с указом президента Российской Федерации от 01 мая 2022 года «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с 1 января 2025 года российским организациям запрещается использовать средства защиты информации, произведенные в определенных иностранных государствах. Несмотря на ограничения, выбор остается большим и зависит от масштабов сети, необходимой пропускной способности, количества подключаемых устройств, управляемости, цены и т.д. При проектировании защищенной корпоративной сети следует выбирать роутеры, которые поддерживают VPN протоколы, на основе которых планируется организация сети и поддерживается шифрование пакетов.

Межсетевые экраны должны обладать возможностью фильтрации и анализа безопасности; для защиты от несанкционированного доступа рекомендуется использовать файрволы с функциями DPI (Deep Packet Inspection) и IDS/IPS (Intrusion Detection and Prevention System). Очевидно, что подбираемый межсетевой экран должен иметь сертификат ФСТЭК России. Различные технологии сетевой защиты и комплексную безопасность обеспечивают NGFW [11].

Необходимо упомянуть и о безопасной и грамотной организации структурированной кабельной системы. Рекомендуется подключение сетевых устройств через сменные патч-корды и витую пару категории 5е, проложенную в защищённых каналах и кабелепроводах (например, для связи между коммутаторами). Прокладка кабелей осуществляется по лоткам и кабельным каналам с поворотами до 90°, с использованием коммутационных панелей и шкафов. На рабочих местах используются сетевые розетки с двумя телекоммуникационными разъемами, подключённые к коммутационным панелям через патч-корды RJ-45, что обеспечивает гибкость и структурированность подключения.

При выборе сетевого оборудования для удаленных сотрудников следует учитывать поддержу VLAN для сегментации сети и управления доступом, возможность работы с несколькими интернет-каналами, включая LTE, для обеспечения бесперебойной работы, а также наличие функций централизованного управления и мониторинга. Кроме того, оборудование должно поддерживать удаленное обновление прошивки и администрирование для обеспечения безопасности VPN-сети и своевременного устранения уязвимостей.

2.5. Разработка политик безопасности

Политика безопасности организации при проектировании КС с применением VPN является одним из ключевых моментов. Не существует единой политики безопасности, разрабатывать ее необходимо под конкретную организацию и внедрять на различных уровнях. Однако существует ряд общих требований:

- использование надежных протоколов, поддерживающих актуальные алгоритмы шифрования;
- постоянное обновление и исправление ошибок ПО, выпускаемого поставщиками оборудования;
- использование антивирусных средств защиты и их постоянная поддержка;
- грамотная настройка контроля доступа, основанная на принципе разумной достаточности;
- настройка и постоянная поддержка списков контроля доступа, чтобы разрешать или блокировать трафик для определенных протоколов;
- отключение неиспользуемых служб;
- настройка портов (для ненужных служб должны быть заблокированы на рабочих станциях, за исключением необходимых служб, таких, как HTTP и HTTPS);
- мониторинг и аудит трафика и событий безопасности.

Данный перечень можно продолжать довольно долго, однако без обучения сотрудников и наложения обязательств на них о неразглашении конфиденциальной информации защита сети не будет реализована в полном объёме. С каждым сотрудником организации необходимо заключать соглашение о неразглашении сведений конфиденциального характера. Сотрудники несут ответственность за соблюдение требований информационной безопасности, будучи

осведомлёнными о соответствующих правилах и политиках, связанных с их профессиональной деятельностью. Несоблюдение этих требований влечёт дисциплинарные меры вплоть до увольнения. Руководители подразделений также обязаны обеспечивать информирование и обучение сотрудников по вопросам безопасности, а также контролировать выполнение этих требований. В случае нарушений они несут ответственность и могут подвергнуться соответствующим санкциям. Нарушения информационной безопасности регулируются внутренними документами организации и законодательством РФ, что может включать расследование инцидента, административные и юридические последствия, а также профилактические меры для предотвращения повторных нарушений, с целью защиты организации от угроз.

Заключение

Использование технологии VPN является эффективным и безопасным решением для организации удаленных филиалов КС. Для обеспечения безопасности существуют различные методы, однако наибольшая результативность достигается за счет комплексного применения всех представленных методов. Для минимизации рисков компрометации информации, обеспечения целостности и доступности информационных ресурсов предприятия необходимо формировать систему защиты КС на всех этапах, начиная от проектирования, построения и заканчивая постоянным мониторингом и контролем. Как правило, не существует четкого набора требований и критериев для конкретной организации и пользователей, что подчеркивает важность разработки понятной методики построения безопасной КС с применением технологии VPN.

В работе представлена методология построения безопасной КС, в которой используются следующие этапы:

- изучение структуры КС и выбор технологий для связи головной организации и филиалов;
- реализация КС с учётом прав доступа;
- определение расположения серверов, коммутационных шкафов и телекоммуникационных розеток;
- создание логической структуры сети [15];
- подбор активного сетевого оборудования;
- распределение сетевых адресов и подсетей;
- создание физической структуры сети;
- разработка политик безопасности, списков доступа и сценариев их реализации.

Важно отметить, что представленные требования могут меняться в зависимости от различных факторов, однако ключевые принципы, описанные выше, остаются неизменными. Представленные этапы построения КС можно использовать в качестве методики для организации удаленных филиалов организаций.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь
DOI: https://doi.org/10.60797/IRJ.2025.153.44.5

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus
DOI: https://doi.org/10.60797/IRJ.2025.153.44.5

Список литературы / References

1. Паньшин Б. Цифровая экономика: понятия и направления развития / Б. Паньшин // Наука и инновации. — 2019. — № 3 (193).
2. Утечки данных больно бьют по капиталу // Системный администратор. — 2023. — Vol. 9. — № 250. — P. 24–25.
3. Средства защиты ПДн: что могут наши ИБ-решения? // Системный администратор. — 2023. — Vol. 10. — № 251. — P. 15–29.
4. Касимова А.Р. Использование цифрового двойника в задачах управления информационной безопасностью / А.Р. Касимова, В.В. Золотарев, Л.Х. Сафиуллина [и др.] // Прикаспийский журнал: управление и высокие технологии. — 2023. — № 1 (61). — С. 48–58. — DOI: 10.54398/20741707_2023_1_48. — EDN: GVJYUN.
5. Корякин С.В. Аналитический обзор методов реализации подсистем удаленного доступа к защищенной корпоративной сети с применением технологий VPN / С.В. Корякин, К.Д. Темурович, И.В. Якимчук [и др.] // The World Of Science and Education. — 2024. — № 20.
6. Al-Fayoumi M. VPN and Non-VPN Network Traffic Classification Using Time-Related Features / M. Al-Fayoumi, M. Al-Fawa’reh, S. Nashwan // Computers, Materials & Continua. — 2022. — Vol. 72. — № 2. — P. 3091–3111.
7. Пиков В.А. Обоснование потребности в разработке методики выбора средств защиты информации для реализации системы защиты информации от несанкционированного доступа / В.А. Пиков, В.А. Кайгородова, О.В. Батманова // Вопросы защиты информации. — 2022. — № 1 (136). — С. 11–16. — DOI: 10.52190/2073-2600_2022_1_11. — EDN: GLRJGD.
8. Голембиовская О.М. Формализация подхода к определению актуальности угроз информационной безопасности / О.М. Голембиовская, М.Ю. Рытов, М.М. Голембиовский [и др.]. — Саратов : Вузовское образование, 2022. — 147 с. — EDN: DIQCQK.
9. Dautbayeva A. Research of vpn general models limited in network resources / A. Dautbayeva [et al.] // KazATK Bulletin. — 2024. — Vol. 130. — № 1. — P. 278–285.

10. Andriani R. Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol / R. Andriani, A. Sa'di, A.D. Putra // Building of Informatics, Technology and Science (BITS). — 2022. — Vol. 4. — № 1.

11. Чайка Е.М. Обзор криптошлюзов для защиты информации в корпоративных сетях / Е.М. Чайка, С.П. Белов // Научный результат. Информационные технологии. — 2024. — № 1.

12. Rusakova E.V. Life cycle of information systems: Models, comparative analysis of different approaches / E.V. Rusakova, M.A. Bystrov // Economics and Entrepreneurship. — 2023. — № 11 (160). — P. 877–881.

13. Шаньгин В.Ф. Информационная безопасность и защита информации : учебное пособие / В.Ф. Шаньгин. — Москва : ДМК Пресс, 2017. — 703 с.

14. Москвин Э.К. Локальная сеть без проводов / Э.К. Москвин. — М.: НТ Пресс, 2021. — 128 р.

15. Гибадуллин Р.Ф. Анализ параметров промышленных сетей с применением нейросетевой обработки / Р.Ф. Гибадуллин, Д.В. Лекомцев, М.Ю. Перухин // Искусственный интеллект и принятие решений. — 2020. — № 1. — С. 80–87. — DOI: 10.14357/20718594200108.

Список литературы на английском языке / References in English

1. Pan'shin B. Cifrovaja jekonomika: ponjatija i napravlenija razvitija [Digital economy: concepts and directions of development] / B. Pan'shin // Nauka i innovacii [Science and Innovations]. — 2019. — № 3 (193). [in Russian]

2. Utechki dannyh bol'no b'jut po kapitalu [Data leaks are hurting capital] // Sistemnyj administrator [System Administrator]. — 2023. — Vol. 9. — № 250. — P. 24–25. [in Russian]

3. Sredstva zashhity PDn: chto mogut nashi IB-reshenija? [Data protection tools: what can our IS solutions do?] // Sistemnyj administrator [System Administrator]. — 2023. — Vol. 10. — № 251. — P. 15–29. [in Russian]

4. Kasimova A.R. Ispol'zovanie cifrovogo dvojnika v zadachah upravlenija informacionnoj bezopasnost'ju [The use of digital twin in the tasks of information security management] / A.R. Kasimova, V.V. Zolotarev, L.H. Safiullina [et al.] // Prikaspijskij zhurnal: upravlenie i vysokie tehnologii [Caspian Journal: Management and High Technologies]. — 2023. — № 1 (61). — P. 48–58. — DOI: 10.54398/20741707_2023_1_48. — EDN: GVJYUN. [in Russian]

5. Korjakin S.V. Analiticheskij obzor metodov realizacii podsistem udalennogo dostupa k zashhishhennoj korporativnoj seti s primeneniem tehnologij VPN [Analytical review of methods of realisation of subsystems of remote access to the protected corporate network with application of VPN technologies] / S.V. Korjakin, K.D. Temurovich, I.V. Jakimchuk [et al.] // The World Of Science and Education. — 2024. — № 20. [in Russian]

6. Al-Fayoumi M. VPN and Non-VPN Network Traffic Classification Using Time-Related Features / M. Al-Fayoumi, M. Al-Fawa'reh, S. Nashwan // Computers, Materials & Continua. — 2022. — Vol. 72. — № 2. — P. 3091–3111.

7. Pikov V.A. Obosnovanie potrebnosti v razrabotke metodiki vybora sredstv zashhity informacii dlja realizacii sistemy zashhity informacii ot nesankcionirovannogo dostupa [Substantiation of the necessity to develop a methodology for selecting information protection means to implement the system of information protection from unauthorised access] / V.A. Pikov, V.A. Kajgorodova, O.V. Batmanova // Voprosy zashhity informacii [Information Protection Problems]. — 2022. — № 1 (136). — P. 11–16. — DOI: 10.52190/2073-2600_2022_1_11. — EDN: GLRJGD. [in Russian]

8. Golembiovskaja O.M. Formalizacija podhoda k opredeleniju aktual'nosti ugroz informacionnoj bezopasnosti [Formalisation of the approach to determining the relevance of information security threats] / O.M. Golembiovskaja, M.Ju. Rytov, M.M. Golembiovskij [et al.]. — Saratov : University Education, 2022. — 147 p. — EDN: DIQCQK. [in Russian]

9. Dautbayeva A. Research of vpn general models limited in network resources / A. Dautbayeva [et al.] // KazATK Bulletin. — 2024. — Vol. 130. — № 1. — P. 278–285.

10. Andriani R. Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol / R. Andriani, A. Sa'di, A.D. Putra // Building of Informatics, Technology and Science (BITS). — 2022. — Vol. 4. — № 1.

11. Chajka E.M. Obzor kriptoshljuzov dlja zashhity informacii v korporativnyh setjah [Review of crypto-gateways for information protection in corporate networks] / E.M. Chajka, S.P. Belov // Nauchnyj rezul'tat. Informacionnye tehnologii [Scientific Result. Information technologies]. — 2024. — № 1. [in Russian]

12. Rusakova E.V. Life cycle of information systems: Models, comparative analysis of different approaches / E.V. Rusakova, M.A. Bystrov // Economics and Entrepreneurship. — 2023. — № 11 (160). — P. 877–881.

13. Shan'gin V.F. Informacionnaja bezopasnost' i zashhita informacii : uchebnoe posobie [Information security and information defence : textbook] / V.F. Shan'gin. — Moscow : DMK Press, 2017. — 703 p. [in Russian]

14. Moskvin Je.K. Lokal'naja set' bez provodov [Local network without wires] / Je.K. Moskvin. — M.: NT Press, 2021. — 128 p. [in Russian]

15. Gibadullin R.F. Analiz parametrov promyshlennyh setej s primeneniem nejrosetevoj obrabotki [Analysis of industrial networks parameters using neural network processing] / R.F. Gibadullin, D.V. Lekomcev, M.Ju. Peruhin // Iskusstvennyj intellekt i prinjatie reshenij [Artificial Intelligence and Decision-Making]. — 2020. — № 1. — P. 80–87. — DOI: 10.14357/20718594200108. [in Russian]