

# Обзор архитектуры безопасности версии 1.0

## 1. Краткий обзор

Непрерывно изменяющаяся ситуация в сфере информационной безопасности постоянно ставит перед организациями новые задачи. Быстрое распространение ботнетов, постоянное усложнение сетевых атак, тревожащий рост организованной киберпреступности и шпионажа с использованием Интернета, хищение персональных и корпоративных данных, более сложные способы инсайдерских атак, развитие новых форм угроз для мобильных систем — вот лишь несколько примеров многообразия и сложности реальных угроз, формирующих современный ландшафт безопасности.

Поскольку сети являются ключевым механизмом ведения бизнеса, при их проектировании и реализации необходимо учитывать проблемы безопасности, чтобы гарантировать конфиденциальность, целостность и доступность данных и системных ресурсов, поддерживающих основные бизнес-функции. Новая архитектура безопасности Cisco предоставляет рекомендации по разработке и внедрению безопасных и надежных сетевых инфраструктур, которые подтвердили свою устойчивость к воздействию как хорошо известных, так и совершенно новых видов атак.

В наши дни для достижения приемлемого уровня безопасности уже не достаточно развернуть точечные продукты на периметре сети. Сложность и изощренность современных угроз требует внедрения интеллектуальных совместно работающих механизмов безопасности во все элементы распределенной инфраструктуры. С учетом этих соображений новая архитектура корпорации Cisco использует подход глубокой многоуровневой защиты (Defense in Depth, или "эшелонированная оборона"), согласно которому множество уровней защиты распределены по стратегически важным элементам по всей сети и действуют в рамках унифицированной стратегии. Информация о событиях и состоянии систем согласованно используется различными элементами системы информационной безопасности, что позволяет обеспечить более надежный контроль состояния ИТ-инфраструктуры, а ответные действия координируются в рамках общей стратегии управления.

В архитектуре предусмотрен модульный принцип построения системы информационной безопасности, что позволяет ускорить развертывание и способствует внедрению новых решений и технологий по мере развития потребностей бизнеса. Такая модульность расширяет срок использования имеющегося оборудования и обеспечивает защиту произведенных капитальных вложений. В то же время архитектура предусматривает набор инструментальных средств, упрощающих повседневную эксплуатацию и обеспечивающих снижение совокупных эксплуатационных расходов.

Разработанная Cisco архитектура основана на концепции Cisco Security Framework, которая обуславливает выбор продуктов и функций, обеспечивающих максимальный уровень безопасности, контроля и управления ИТ-инфраструктурой. Эта концепция также используется при оказании услуг Cisco в течение жизненного цикла решения и способствует интеграции широкого спектра услуг Cisco в области информационной безопасности, предназначенных для поддержки продукта на протяжении всего жизненного цикла.

В данном документе представлен обзор новой архитектуры Cisco, обеспечивающей безопасность корпоративных сетей — Security Architecture for Enterprise Networks (SAFE). Хотя материал предназначен для лиц, принимающих бизнес-решения, высших руководителей ИТ-подразделений и системных архитекторов, в документе также описаны основы архитектуры и дизайна, которые могут заинтересовать технических специалистов.

## 2. Концепция Cisco Security Framework

Концепция Cisco Security Framework (CSF) представляет собой концепцию создания системы информационной безопасности, ориентированной на обеспечение доступности сети и сервисов и поддержание непрерывности бизнеса. Угрозы безопасности характеризуются высокой динамикой, и концепция CSF предусматривает способы выявления текущих направлений угроз, а также отслеживания новых и развивающихся угроз за счет следования лучшим практическим рекомендациям и использования комплексных решений. Новая архитектура системы безопасности Cisco использует подходы, определенные в концепции CSF, для определения продуктов и функций, позволяющих надежно обеспечить безопасность во всей сети.

Концепция CSF предполагает наличие политик безопасности, разработанных по результатам анализа угроз и рисков и согласованных с бизнес-целями и задачами. Критически важным фактором для достижения успеха бизнеса является создание таких политик безопасности, которые не только не препятствуют, а, напротив, способствуют достижению организацией поставленных бизнес-целей и плановых показателей. Поэтому разработка политик должна начинаться с четкого определения бизнес-целей и задач. После определения этих целей, необходимо выявить возможные угрозы для выделенных целей и задач. В таблице 1 представлены некоторые типовые примеры бизнес-целей и задач, а также связанные с ними возможные угрозы. Следует иметь в виду, что цели, задачи и возможные угрозы могут сильно меняться в зависимости от организации и среды, данный перечень приводится только в качестве примера.

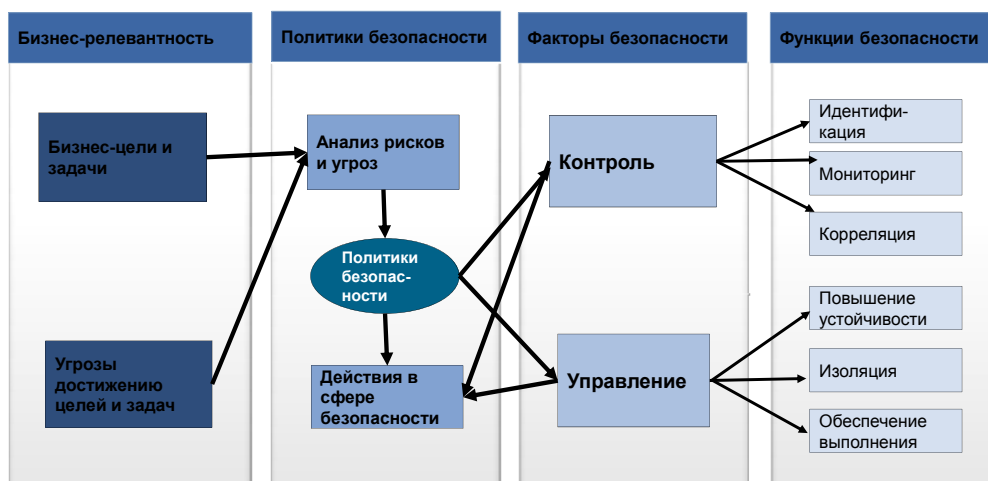
**Таблица 1.** Бизнес-цели, задачи и возможные угрозы

Бизнес-цели и задачи	Возможные угрозы
Защита источников дохода	Прерывание бизнеса вследствие нарушения безопасности может повлечь за собой немедленные и долговременные потери доходов.
Соответствие требованиям заказчиков	Несоответствие ожиданиям заказчиков в части конфиденциальности, безопасности и уровней обслуживания может привести к серьезным убыткам.
Защита корпоративной идентификационной информации и бренда	Раскрытие конфиденциальных данных может разрушить тщательно спланированные маркетинговые кампании и повредить репутации бренда.
Соблюдение требований нормативных документов и стандартов	Недостаточное соответствие нормативно-правовым требованиям может привести к отзыву лицензий, потере бизнеса, денежным взысканиям и к более серьезным юридическим последствиям.

После определения бизнес-целей и задачи и проведения анализа угроз необходимо выполнить более глубокий анализ угроз и рисков, чтобы определить важность ресурсов, имеющихся в среде, проанализировать возможные риски безопасности для этих ресурсов, а также оценить возможное воздействие нарушений безопасности на бизнес. Таким образом, будет сформировано представление об усилиях, необходимых для защиты каждого ресурса.

Результатом этих шагов является создание политик безопасности и формулирование принципов, которыми определяется приемлемое и безопасное использование каждого сервиса, устройства и системы в рамках ИТ-инфраструктуры организации. В свою очередь, политики безопасности определяют процессы и процедуры, необходимые для достижения бизнес-целей и выполнения задач. Совокупность процессов и процедур определяет операции по обеспечению безопасности. Эти понятия проиллюстрированы на рис. 1.

Рисунок 1. Графическое представление концепции Cisco Security Framework



Результат, обеспечиваемый внедрением политик безопасности, полностью зависит от того, насколько они улучшают контроль и управление. Другими словами, безопасность можно представить как функцию контроля и управления. Без контроля невозможно управление, а без управления нет безопасности. Таким образом, концепция CSF ориентирована главным образом на повышение уровня контроля и управления, которые являются основными факторами успешного обеспечения безопасности. На практике концепция CSF определяет условия и методы выбора и развертывания платформ и функций для достижения требуемого уровня контроля и управления. Ниже указаны примеры мер, которые могут улучшить обеспечение основных факторов безопасности.

Таблица 2. Основные факторы безопасности: контроль и управление

Контроль
<ul style="list-style-type: none"> <li>• Идентификация пользователей, трафика, приложений, протоколов и схем использования ресурсов</li> <li>• Мониторинг и регистрация активности и шаблонов (схем)</li> <li>• Сбор и выявление взаимозависимостей данных, полученных из нескольких источников, для идентификации трендов и событий в масштабе всей системы.</li> <li>• Обнаружение и идентификация аномального трафика и угроз.</li> <li>• Классификация, обеспечивающая применение методов контроля.</li> </ul>
Управление
<ul style="list-style-type: none"> <li>• Повышение уровня защищенности сетевой инфраструктуры.</li> <li>• Ограничение доступа и использования на уровне пользователя, протокола, сервиса и приложения.</li> <li>• Защита от известных угроз и эксплойтов.</li> <li>• Изоляция пользователей, сервисов и приложений.</li> <li>• Динамическая реакция на аномальные события.</li> </ul>

В рамках концепции CSF определены шесть мер обеспечения безопасности, которые обеспечивают выполнение политик безопасности и расширяют возможности по контролю и управлению. Уровень контроля повышается с помощью мер "идентификация", "мониторинг" и "выявление взаимозависимостей". Уровень управления повышается с помощью мер "повышение устойчивости", "изоляция" и "обеспечение выполнения политик".

Таблица 3. Меры обеспечения безопасности

Контроль	Идентификация	Идентификация и классификация пользователей, сервисов, трафика и конечных устройств.
	Мониторинг	Мониторинг производительности, поведения, шаблонов использования, событий и соответствия политике.
	Выявление взаимозависимостей	Сбор, анализ и выявление взаимозависимостей событий в масштабе системы.
Управление	Повышение устойчивости	Повышение устойчивости конечных устройств, сервисов, приложений и инфраструктуры.
	Изоляция	Изоляция пользователей, систем и сервисов для сдерживания и защиты.
	Обеспечение выполнения	Обеспечение выполнения политики разграничения доступа, политик безопасности и противодействие угрозам безопасности.

В контексте новой архитектуры безопасности концепция CSF используется при создании каждого сегмента сети. Результатом следования концепции CSF является идентификация технологий и лучших типовых практических рекомендаций для выполнения каждой из шести ключевых мер, которые наиболее подходят для данной среды. Таким образом, многочисленные технологии и функции используются в масштабе всей сети и обеспечивают контроль сетевых операций, реализуют сетевую политику и направлены на разрешение проблем, связанных с обработкой аномального трафика. Элементы сетевой инфраструктуры, такие как маршрутизаторы и коммутаторы, используются в качестве средств всеобъемлющего упреждающего мониторинга и обеспечения выполнения политики.

Учитывая постоянно растущие потребности бизнеса и безопасности, концепция CSF предусматривает непрерывный анализ и корректировку реализации системы информационной безопасности. С этой целью концепция CSF регламентирует эволюционный жизненный цикл решения в сфере информационной безопасности, который показан на рисунке 2.

Рисунок 2. Жизненный цикл CSF



Цикл начинается с планирования, которое должно включать анализ угроз и рисков с целью идентификации ресурсов и текущего состояния безопасности. В ходе этапа планирования также должен выполняться анализ недостатков существующего решения, что позволяет выявить сильные стороны и слабые места существующей архитектуры. По окончании начального планирования цикл продолжается этапом проектирования и выбора платформ, функций и практических рекомендаций, необходимых для устранения недостатков и удовлетворения будущих потребностей. Результатом этого этапа является создание подробного проекта, удовлетворяющего бизнес-потребностям и техническим требованиям. За этапом проектирования следует этап внедрения. Он включает развертывание и подготовку к работе платформ и функций. Как правило, развертывание выполняется в несколько отдельных этапов, что требует формализации

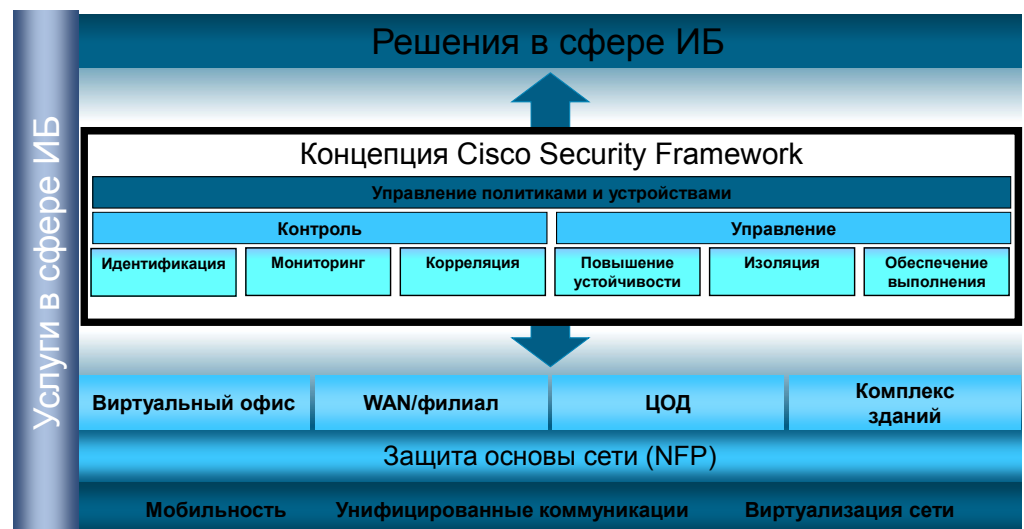
последовательности действий в рамках плана. После окончания развертывания начинается эксплуатация и обслуживание развернутого решения. Этот этап включает действия по управлению инфраструктурой и мониторингу ее состояния, а также сбор информации в области информационной безопасности для отражения угроз. Наконец, поскольку требования бизнеса и безопасности постоянно изменяются, необходимо проводить регулярный аудит системы информационной безопасности, чтобы обнаруживать и устранять возможные недостатки. Для этих целей может использоваться информация, получаемая как в ходе повседневной эксплуатационной деятельности, так и в результате специальных проверок.

Как показано на рисунке 2, процесс является итерационным, и результатом каждой итерации является разработка более совершенной архитектуры, позволяющей удовлетворить требования бизнеса и политики безопасности.

### 3. Архитектура безопасности

В новой архитектуре безопасности реализована модель глубокой эшелонированной обороны, которая предусматривает размещение решений и средств Cisco для обеспечения информационной безопасности в стратегически важных точках сети и активное взаимодействие между различными платформами. Широкий спектр технологий безопасности функционирует на нескольких уровнях сети, но в соответствии с общей согласованной стратегией и под управлением одного администратора. Решения и средства для обеспечения информационной безопасности размещаются в тех точках сети, в которых они приносят максимальную пользу с учетом требований к совместной работе сетевых элементов и простоте эксплуатации. Новая архитектура безопасности Cisco представлена на рисунке 3.

Рисунок 3. Архитектура безопасности Cisco



Архитектура безопасности Cisco предоставляется в виде шаблонов дизайна и решений для обеспечения информационной безопасности:

- **Шаблоны дизайна – дизайны, рекомендуемые Cisco (Cisco Validated Design, CVD), и руководства, содержащие практические рекомендации в области информационной безопасности.** Методические указания по проекту предоставляются в виде руководств по рекомендуемым дизайнам, ориентированным на различные сегменты корпоративной сети, например, сети комплекса зданий, сегменты периметра при подключении локальной сети к глобальной сети, сети филиалов и сети центра обработки данных. Руководящие указания по дизайну также предоставляются для технологий или элементов, распределенных по сети, таких как система унифицированных коммуникаций, средства виртуализации сети и система

защиты основных сетевых элементов. В рамках этих дизайнов выбор платформ и функций определяется концепцией Cisco Security Framework.

- **Решения для обеспечения информационной безопасности.** Концепция Cisco Security Framework и шаблоны дизайна позволяют сформировать основу для последующего создания вертикальных и горизонтальных решений для обеспечения информационной безопасности. Эти решения для обеспечения информационной безопасности соответствуют требованиям конкретной отрасли, например, розничной торговли, финансовой сферы, здравоохранения и производственной промышленности.

Как показано на рисунке 3, услуги Cisco по обеспечению информационной безопасности являются неотъемлемой частью архитектуры. Услуги Cisco по обеспечению информационной безопасности обеспечивают поддержку решений в течение всего их жизненного цикла и разнообразных продуктов, используемых в шаблонах архитектуры.

### 3.1. Сценарии использования в масштабах всей сети

Корпоративные сети являются гетерогенными средами, которые состоят из разнообразных блоков и в которых используется множество технологий. Данная версия архитектуры ориентирована на большинство базовых и общих сценариев использования. Некоторые из этих сценариев использования применимы к сети в целом, в то время как другие применимы только к отдельным сегментам сети. Прочие сценарии использования будут рассмотрены в последующих выпусках документации.

Данная версия архитектуры ориентирована на следующие сценарии использования в масштабах всей сети:

- защита основы сети (SNF);
- отслеживание, анализ и выявление взаимозависимостей событий;
- управление угрозами и противодействие угрозам.

Услуги Cisco по обеспечению информационной безопасности на протяжении жизненного цикла, применяемые в этих сценариях использования, включают планирование технологий обеспечения безопасности, контроль развертывания сети, оценку состояния защищенности, анализ архитектуры системы безопасности, развертывание и миграцию продуктов, подписку на контент и услуги по оптимизации. Более подробная информация об услугах Cisco по обеспечению информационной безопасности представлена в главе 6.

#### 3.1.1 Защита основы сети

Корпоративные сети строятся на основе маршрутизаторов, коммутаторов и других сетевых устройств, которые обеспечивают работу приложений и сервисов. Поэтому обеспечение надлежащей защиты этих сетевых устройств имеет критически высокое значение для обеспечения непрерывности бизнеса. Сетевая инфраструктура не только нередко используется в качестве платформы для проведения атаки, но и все чаще становится прямой целью вредоносных действий. По этой причине необходимо предпринять все возможные меры по обеспечению безопасности, надежности и доступности сетевой инфраструктуры.

Архитектура безопасности предоставляет рекомендованные дизайны для обеспечения повышенного уровня безопасности и передовые рекомендации по защите уровней контроля и управления инфраструктурой. Архитектура позволяет сформировать надежную основу, на которой впоследствии могут использоваться более перспективные методы и технологии.

Передовые рекомендации и советы по дизайну предоставляются в следующих областях:

- доступ к устройствам, формирующим инфраструктуру;
- отказоустойчивость и бесперебойная работа устройств;
- инфраструктура маршрутизации;
- инфраструктура коммутации;
- обеспечение выполнения сетевой политики;

- сетевая телеметрия;
- сетевое управление.

Подробные дизайны и передовые рекомендации по защите основы сети представлены в документе Network Security Baseline, доступном по адресу:

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline\\_Security/securebasebook.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html)

### 3.1.2 Отслеживание, анализ и выявление взаимозависимостей событий

С увеличением уровня сложности атак точечные решения для обеспечения безопасности перестают быть эффективными. Современная среда требует более высокого уровня контроля, который достигается только при внедрении совместно работающих средств безопасности и сбора информации в области безопасности в масштабе всей сетевой инфраструктуры. Поэтому для обеспечения постоянного контроля сетевых операций в новой архитектуре системы безопасности используются различные средства сетевой телеметрии, имеющиеся в сетевом оборудовании, устройствах защиты и оконечных устройствах. Сбор информации о событиях безопасности и выявление тенденций и взаимозависимостей между событиями безопасности осуществляются на основании данных журналов событий и отдельных событий, которые формируются маршрутизаторами, коммутаторами, межсетевыми экранами, системами обнаружения вторжений и программным обеспечением для защиты оконечных устройств. В архитектуре также используются механизмы совместной работы различных платформ безопасности, например, систем обнаружения вторжений, межсетевых экранов и программного обеспечения для защиты оконечных устройств.

За счет использования распределенных интеллектуальных механизмов безопасности и сбора информации в области безопасности в масштабе всей ИТ-инфраструктуры архитектура системы информационной безопасности позволяет эффективно решать следующие задачи:

- **Идентификация угроз.** Сбор данных и выявление тенденций и взаимозависимостей между событиями безопасности на основании журналов событий, информации о потоках данных и отдельных событий позволяет обнаруживать угрозы безопасности и утечки данных.
- **Подтверждение нарушений безопасности.** Средства отслеживания атаки по мере ее распространения по сети и контроля процессов на оконечных устройствах позволяют архитектуре надежно определять результативность атаки (успех или провал).
- **Снижение количества ложных срабатываний.** Средства контроля оконечных устройств и систем позволяют определить, действительно ли цель является уязвимой для данной атаки.
- **Снижение объема информации о событиях.** Средства выявления взаимозависимостей событий радикально снижают количество элементарных событий безопасности, что позволяет сэкономить время операторов системы безопасности и дает им сосредоточиться на решении важных задач.
- **Динамическая корректировка уровня серьезности инцидента.** Благодаря улучшенным средствам контроля оконечных устройств и сети архитектура способна повысить или понизить уровень серьезности инцидента в соответствии со степенью уязвимости цели и контекстом атаки.

### 3.1.3. Контроль и отражение угроз

Архитектура Cisco основана на совместной работе всех элементов системы информационной безопасности и сборе информации в масштабе всей инфраструктуры, обеспечиваемых продуктами Cisco для контроля и отражения хорошо известных и совершенно новых атак. В рамках этой архитектуры системы обнаружения вторжений, межсетевые экраны, системы контроля доступа к сети, программное обеспечение оконечных устройств и системы мониторинга и анализа работают совместно, чтобы идентифицировать угрозы и динамически реагировать на них. Архитектура способна идентифицировать источник угрозы, визуально представить путь распространения атаки

и предложить ответные действия или даже динамически реализовать их. Варианты ответных действий включают изоляцию систем, безопасность которых нарушена, ограничение пропускной способности, сброс соединений, фильтрацию пакетов, фильтрацию по адресу отправителя и прочие меры.

Ниже перечислены некоторые цели внедрения решения по управлению и противодействию угрозам.

- Полный контроль. Сбор данных в рамках всей ИТ-инфраструктуры организации обеспечивает точное представление топологии сети, путей распространения угроз и позволяет сформировать точное представление об ущербе.
- Адаптивная реакция на угрозы в режиме реального времени. Динамическая идентификация и блокирование угроз осуществляются в режиме реального времени.
- Последовательное применение политики. В соответствии с моделью эшелонированной обороны меры по отражению и сдерживанию угроз могут быть реализованы в различных сегментах сети.
- Снижение ущерба от атак. Ответные действия могут быть предприняты немедленно после обнаружения угрозы, что сводит ущерб к минимуму.
- Единые средства управления политиками и безопасностью. Единая платформа управления политиками и безопасностью упрощает контроль и администрирование, а также снижает эксплуатационные расходы.

### 3.2. Сценарии использования у заказчиков

В дополнение к сценариям использования в масштабе всей сети, описанным в предыдущих разделах, данная версия архитектуры ориентирована на следующие специфические сценарии использования для конкретных сегментов сети:

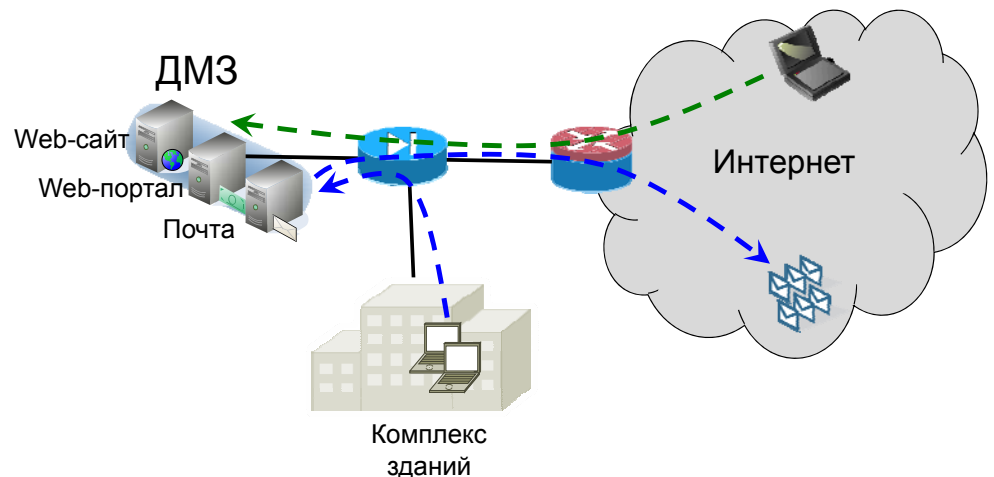
- демилитаризованная зона для общедоступных сервисов;
- корпоративный доступ в Интернет;
- сети VPN для удаленного доступа;
- защищенные каналы связи по глобальной сети;
- защищенная сеть филиала;
- защищенная сеть комплекса зданий;
- центр обработки данных в сети интранет.

Услуги Cisco по обеспечению информационной безопасности на протяжении жизненного цикла, применяемые в этих сценариях использования, включают планирование технологий обеспечения безопасности, контроль развертывания сети, оценку состояния защищенности, анализ архитектуры системы безопасности, развертывание и миграцию продуктов, подписку на контент и услуги по оптимизации. Более подробная информация об услугах по обеспечению информационной безопасности представлена в главе 6.

#### 3.2.1. Демилитаризованная зона для общедоступных сервисов

В целях обеспечения безопасности и контроля общедоступные сервисы обычно размещаются в демилитаризованной зоне (ДМЗ). ДМЗ выступает в роли промежуточной области между Интернетом и закрытыми ресурсами организации и предотвращает доступ внешних пользователей к внутренним серверам и данным. Как показано на рисунке 4, сервисы, развернутые в ДМЗ, часто включают веб-сайт организации, портал для доступа партнеров, сервер электронной почты, FTP-сервер, DNS-сервер и прочие сетевые сервисы.

Рисунок 4. Топология ДМЗ



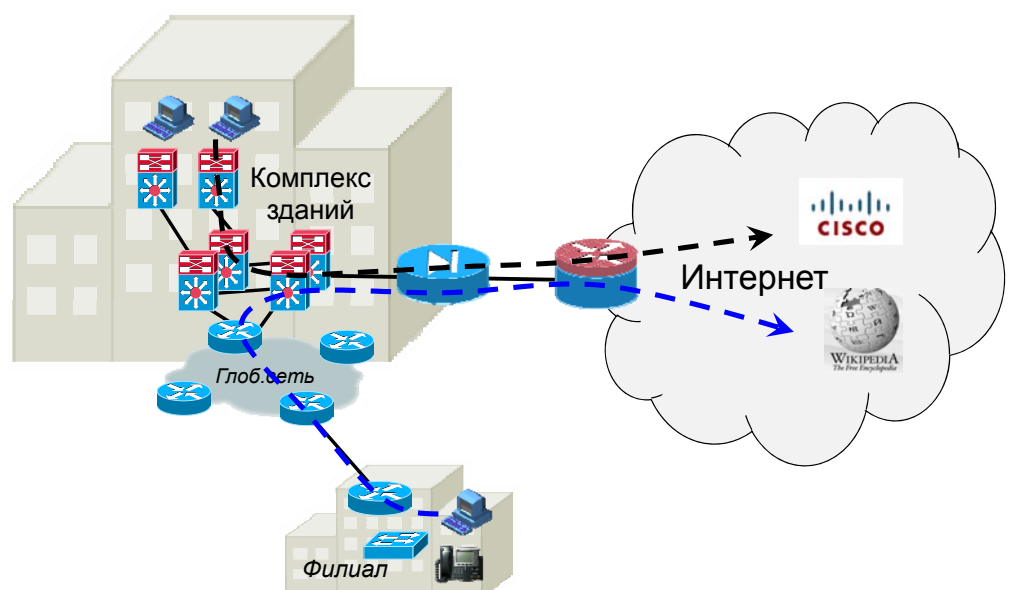
Ниже перечислены некоторые ключевые характеристики безопасности, которые должна обеспечивать структура сети ДМЗ:

- доступность и отказоустойчивость сервисов;
- предотвращение вторжений, атак типа "отказ в обслуживании", утечек данных и мошенничества;
- обеспечение конфиденциальности пользователей, целостности и доступности данных;
- защита серверов и приложений;
- сегментация серверов и приложений.

### 3.2.2 Корпоративный доступ в Интернет

Пользователи сети комплекса зданий осуществляют доступ к электронной почте, системам мгновенного обмена сообщениями, ресурсам Интернета и общим сервисам по каналам Интернета, имеющимся в главных или региональных офисах компаний. В зависимости от политики организации, пользователи в филиалах могут осуществлять доступ к Интернету через централизованное Интернет-подключение, обычно поддерживаемое в главных офисах. Сетевая инфраструктура, поддерживающая Интернет-каналы, также известна как периметр корпоративной сети, подключенный к Интернету.

Рисунок 5. Доступ в Интернет



Ниже перечислены некоторые ключевые характеристики безопасности, которые должна обеспечивать структура сети:

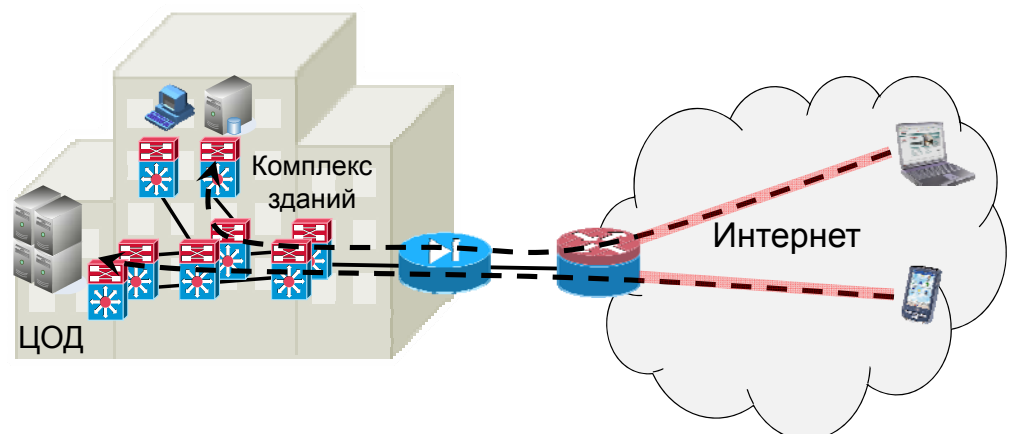
- доступность и отказоустойчивость сервисов;
- предотвращение атак типа "отказ в обслуживании", злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества;
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение сегментации пользователей;
- управление контентом и его анализ.

### 3.2.3. Сети VPN для удаленного доступа

Инфраструктура периметра, подключенного к Интернету, также может предоставлять мобильным пользователям и удаленным работникам доступ к закрытым приложениям и данным, расположенным во внутренней сети организации.

Этот вид удаленного доступа предполагает аутентификацию и выполняется по сети SSL VPN или IPSec VPN. Политики разграничения доступа могут ограничивать доступ только к необходимым ресурсам в соответствии с ролью пользователя. Типовые сервисы, предоставляемые мобильным пользователям и удаленным работникам, включают электронную почту, доступ к web-сайтам в сети интранет, бизнес-приложениям, видео по запросу, системам IP-телефонии, системам мгновенного обмена сообщениями и другим ресурсам корпоративной ИТ-инфраструктуры.

Рисунок 6. Топология сети VPN для удаленного доступа



Ниже перечислены некоторые ключевые характеристики безопасности, которые должна обеспечивать инфраструктура удаленного доступа:

- доступность и отказоустойчивость сервисов;
- предотвращение злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества;
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение сегментации пользователей;
- защита конечных устройств.

### 3.2.4. Защищенные каналы связи по глобальной сети

Удаленные филиалы обычно подключаются к центральным офисам через частную глобальную сеть, иногда находящуюся в собственности предприятия, но чаще предоставляемую провайдером услуг. Для обеспечения резервирования и распределения нагрузки может использоваться несколько каналов глобальной сети. В качестве вспомогательного резервного варианта соединения может использоваться соединение через Интернет.

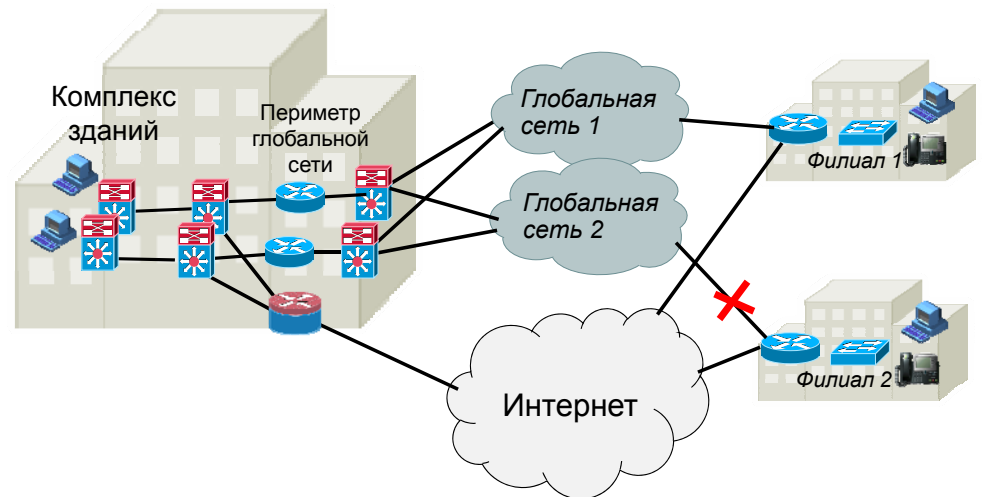


Рисунок 7. Топология периметра, подключенного к глобальной сети

С точки зрения безопасности структура периметра, подключенного к глобальной сети должна обеспечивать следующие ключевые характеристики:

- доступность и отказоустойчивость сервисов;
- предотвращение атак типа "отказ в обслуживании", злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества;
- обеспечение конфиденциальности, целостности и доступности данных, передаваемых через глобальную сеть;
- обеспечение защищенного резервного соединения через Интернет (глобальную сеть);
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение сегментации пользователей.

### 3.2.5. Защищенная сеть филиала

Сети удаленных филиалов предоставляют возможность подключения пользователей и устройств, находящихся на территории филиала. Филиалы обычно используют одну или несколько локальных сетей и могут размещать в своей сети некоторые локальные сервисы передачи данных, голоса и видео.

Как указано выше, сети филиалов подключаются к корпоративной сети через частную глобальную сеть. Для обеспечения резервирования и распределения нагрузки может использоваться несколько каналов глобальной сети.

В дополнение к соединениям с одной или несколькими частными глобальными сетями, удаленные филиалы могут иметь прямое подключение к Интернету. В зависимости от политики доступа организации, доступ в Интернет может быть разрешен из сети филиала или ограничен доступом через централизованное Интернет-подключение, поддерживаемое в главном или региональном офисе компании. В последнем случае Интернет-канал в филиале будет, вероятно, использоваться исключительно в качестве резервного подключения к глобальной сети.

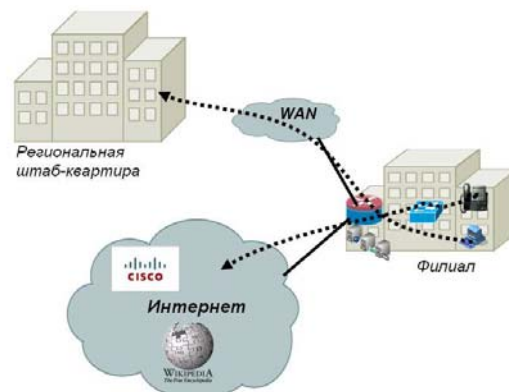


Рисунок 8. Защищенная сеть филиала

Ниже перечислены ключевые характеристики, которые должна обеспечивать сеть филиала:

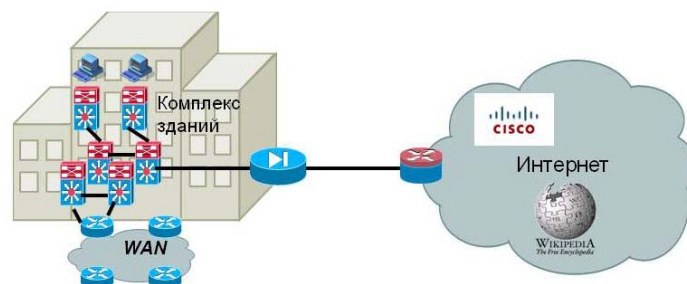
- доступность и отказоустойчивость сервисов;
- предотвращение несанкционированного доступа, злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества;
- обеспечение конфиденциальности, целостности и доступности данных, передаваемых через глобальную сеть;
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение сегментации пользователей;
- защита оконечных устройств.

### 3.2.6. Защищенная сеть комплекса зданий

Сеть комплекса зданий предприятия является частью инфраструктуры, которая предоставляет доступ к сети конечным пользователям и устройствам, расположенным на одной территории. Эта сеть может распространяться на несколько этажей в одном здании или несколько зданий, охватывая более обширную территорию. Сеть комплекса зданий может использоваться для размещения локальных сервисов передачи данных, голоса и видео.

Сеть комплекса зданий обычно подключается к ядру сети, которое обеспечивает доступ к центрам обработки данных, глобальным сетям, другим сетям комплексов зданий и даже к Интернету.

Рисунок 9. Защищенная сеть комплекса зданий



С точки зрения безопасности, структура сети комплекса зданий должна обеспечивать следующие ключевые характеристики:

- доступность и отказоустойчивость сервисов;
- предотвращение несанкционированного доступа, злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества;
- обеспечение конфиденциальности, целостности и доступности данных;
- обеспечение сегментации пользователей;
- применение политики разграничения доступа;
- защита оконечных устройств.

### 3.2.6. Центр обработки данных в сети интранет

Центр обработки данных представляет собой комплекс, в котором размещается большое количество систем, используемых для обслуживания приложений и хранения значительных объемов данных. Понятие ЦОД также распространяется на сетевую инфраструктуру для поддержки функционирования приложений, включая маршрутизаторы, коммутаторы, средства распределения нагрузки, устройства для ускорения работы приложений и прочее оборудование. Центр обработки данных в сети интранет — это центр обработки данных, предназначенный для обслуживания внутренних пользователей и приложений, прямой доступ к нему посторонних пользователей из Интернета невозможен. Центры обработки данных в сети интранет

обычно требуют высокой пропускной способности, поэтому они соединяются с остальной частью сети предприятия через высокоскоростное ядро сети.

**Рисунок 10.** Центр обработки данных в сети интранет



Ниже перечислены некоторые ключевые характеристики безопасности, которые должна обеспечивать структура ЦОД:

- доступность и отказоустойчивость сервисов;
- предотвращение атак типа "отказ в обслуживании", злоупотреблений сетевыми сервисами, вторжений, утечек данных и мошенничества
- обеспечение конфиденциальности, целостности и доступности данных;
- управление контентом и анализ сетевого трафика на уровне приложений;
- защита и сегментация серверов и приложений.

#### 4. Подход к защите основы сети SNF

Эффективная защита сети требует внедрения разнообразных мер безопасности, реализованных в виде многоуровневой системы и управляемых в рамках единой стратегии. С этой целью подробные схемы дизайна архитектуры и решения в области безопасности изначально строятся с учетом требований безопасности. При этом многочисленные технологии и функции, обеспечивающие безопасность, стратегически развертываются в масштабе всей сети, дополняют друг друга и взаимодействуют между собой. Реализуемые в рамках единой стратегии меры безопасности призваны обеспечить максимальный уровень контроля и управления сетью.

В этом разделе документа описаны практические рекомендации по обеспечению безопасности самой инфраструктуры, уровни контроля и управления, создание надежной основы, на которой впоследствии могут быть развернуты более современные методы и технологии. Далее в этом документе каждый сценарий использования будет представлен с дополнительными элементами дизайна, обеспечивающими безопасность и необходимыми для повышения уровня контроля, управления и защиты уровня данных.

Ниже перечислены ключевые области, которые рассматриваются при обеспечении безопасности сети:

- доступ к устройствам, формирующим инфраструктуру;
- инфраструктура маршрутизации;
- устойчивость и безотказная работа устройств;
- сетевая телеметрия;
- обеспечение выполнения сетевой политики;
- инфраструктура коммутации.

Чтобы гарантировать полноту решения, технологии и функции выбираются в соответствии с концепцией Cisco Security Framework (CSF). Концепция CSF регламентирует методику оценки и проверки требований к безопасности системы и предписывает рассмотрение и выбор мер обеспечения безопасности для каждой

конкретной контекстной области. Подробное рассмотрение различных элементов системы защиты основы сети SNF в соответствии с концепцией CSF представлено в документе Network Security Baseline по следующему адресу:

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline\\_Security\\_securebasebook.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security_securebasebook.html)

#### **4.1. Доступ к устройствам, формирующим инфраструктуру**

Защита сетевой инфраструктуры предполагает защиту доступа к устройствам, формирующим инфраструктуру, с целью управления. Если безопасность доступа к устройствам, формирующим инфраструктуру, нарушается, то может быть нарушена и безопасность сети в целом, включая средства сетевого управления. Поэтому критически важно реализовать соответствующие средства контроля и разграничения доступа для предотвращения несанкционированного доступа к устройствам, формирующим инфраструктуру.

Устройства, формирующие сетевую инфраструктуру, нередко поддерживают большое количество различных механизмов доступа, включая консольные и асинхронные соединения, а также возможности удаленного доступа с использованием протоколов Telnet, rlogin, HTTP и SSH. Некоторые механизмы обычно включены по умолчанию, при этом нередко с ними связаны минимальные меры обеспечения безопасности. Например, платформы на основе программного обеспечения Cisco IOS поставляются с включенными по умолчанию консольным и модемным доступом. По этой причине каждое устройство, формирующее сетевую инфраструктуру, должно быть тщательно проверено и настроено, чтобы обеспечить включение только поддерживаемых механизмов доступа и их надлежащую защиту.

Для обеспечения защиты интерактивного доступа и доступа с целью управления к устройствам, формирующим инфраструктуру, используются следующие основные меры:

- Ограничение доступа к устройству. Ограничение доступных портов, ограничение адресов, с которых разрешено подключение, и разрешенных методов доступа.
- Отображение юридического уведомления. Отображение юридического уведомления, разработанного совместно с юридической службой компании, в начале интерактивного сеанса работы с устройством.
- Аутентификация доступа. Предоставление доступа только пользователям, группам и сервисам, прошедшим процедуру аутентификации.
- Ограничение возможностей. Ограничение действий и представлений только теми, которые разрешены для конкретных пользователей, групп и сервисов.
- Обеспечение конфиденциальности данных. Защита важных данных, хранимых на локальных носителях, от просмотра и копирования. Анализ уязвимости данных, передаваемых по коммуникационным каналам, по отношению к методам перехвата пакетов, взлома сеансов и атакам типа "посредник" (MITM).
- Регистрация и учет для всех видов доступа. Регистрация лиц, осуществляющих доступ к устройству, выполняемых операций и времени их выполнения в целях аудита.

#### **4.2. Инфраструктура маршрутизации**

Система маршрутизации является одной из наиболее значимых составляющих инфраструктуры, которая поддерживает работоспособность сети, и поэтому критически важно принять необходимые меры для ее защиты. Существуют различные способы нарушения безопасности системы маршрутизации, от внедрения нелегитимных обновлений маршрутной информации до DoS-атак, целенаправленно проводимых для нарушения маршрутизации. Атаки могут быть направлены непосредственно на маршрутизаторы, на сеансы обмена маршрутной информацией и (или) на саму маршрутную информацию.

Для эффективной защиты уровня маршрутизации в дизайнах архитектуры используются следующие меры:

- Ограничение круга систем, использующих протоколы маршрутизации. Ограничение сеансов маршрутизации только доверенными узлами, проверка происхождения и целостности обновлений маршрутной информации.
- Контроль распространения маршрутной информации. Применение фильтров маршрутизации, чтобы гарантировать распространение только достоверной маршрутной информации. Контроль обмена маршрутной информацией между узлами маршрутизации и между процессами ее перераспределения.
- Регистрация изменений состояния. Регистрация изменений состояния сеансов со смежными или соседними узлами.

#### 4.3. Отказоустойчивость и безотказная работа устройств

Маршрутизаторы и коммутаторы могут подвергаться атакам, которые проводятся для снижения доступности сети либо косвенно сказываются на ней. Среди возможных атак – DoS-атаки с использованием неразрешенных и разрешенных протоколов, распределенные DoS-атаки, атаки «шторма» пакетов (flood-атаки), разведка, несанкционированный доступ и другие виды атак.

Для обеспечения устойчивости и безотказной работы маршрутизаторов и коммутаторов в проектах дизайна предусмотрены следующие практические рекомендации:

- Отключение неиспользуемых сервисов. Отключение сервисов, включенных по умолчанию, которые не требуются для работы.
- Ограничение доступа адресным пространством инфраструктуры сети. Развертывание списков ACL на периметре сети для защиты инфраструктуры от несанкционированного доступа, DoS-атак и других видов сетевых атак.
- Защита уровня управления. Фильтрация и ограничение трафика, направленного на уровень управления маршрутизаторов и коммутаторов.
- Контроль использования памяти коммутаторов, адресуемой по содержимому. Ограничение списка MAC-адресов, имеющих право отправлять трафик на определенный порт.
- Резервирование. Исключение единственных точек отказа путем резервирования интерфейсов, развертывания резервных устройств в режиме ожидания и топологической избыточности.

#### 4.4. Сетевая телеметрия

Для успешной эксплуатации и поддержания бесперебойной работы сети важно обеспечить контроль процессов, происходящих в сети, и возможность управлять функционированием сети в любой момент времени. Средства сетевой телеметрии предоставляют развитые и удобные функции обнаружения событий, которые могут использоваться в сочетании со специализированными системами анализа для сбора данных и выявления тенденций и взаимозависимостей регистрируемых событий.

В данном разделе рассматриваются основные виды телеметрии, рекомендованные для устройств, формирующих сетевую инфраструктуру.

- Синхронизация времени. Внедрение протокола NTP (Network Time Protocol), обеспечивающего синхронизацию отметок даты и времени в журналах регистрации и оповещениях.
- Ведение статистики локального трафика устройства. Использование статистических сведений об общем трафике устройства и трафике для отдельных интерфейсов.
- Сбор информации о состоянии системы. Использование информации о состоянии памяти, ЦП и процессов.
- Системный журнал. Сбор и регистрация информации о состоянии системы, статистике трафика и доступе к устройству.

- Регистрация и учет для всех видов доступа. Регистрация лиц, осуществляющих доступ к устройству, происходящих событий и времени их выполнения для целей аудита.
- Сбор пакетов. Создание механизмов, позволяющих собирать передаваемые через устройство пакеты, для анализа и статистики.

#### 4.5. Обеспечение выполнения сетевой политики

Обеспечение выполнения основных сетевых политик касается главным образом трафика, поступающего в сеть. Этот трафик должен соответствовать сетевой политике, включая диапазон IP-адресов и типы трафика. Аномальные пакеты должны отбрасываться как можно ближе к периметру сети, что позволяет снизить риск их нежелательного воздействия до минимума.

В проектах дизайна предусмотрены следующие меры:

- Фильтрация на периметре сети. Обработка трафика, адресованного в пространство инфраструктуры.
- Защита от подмены IP-адресов отправителей. Внедрение фильтрации пакетов и других динамических механизмов для блокирования пакетов с подмененными IP-адресами отправителей.

#### 4.6. Инфраструктура коммутации

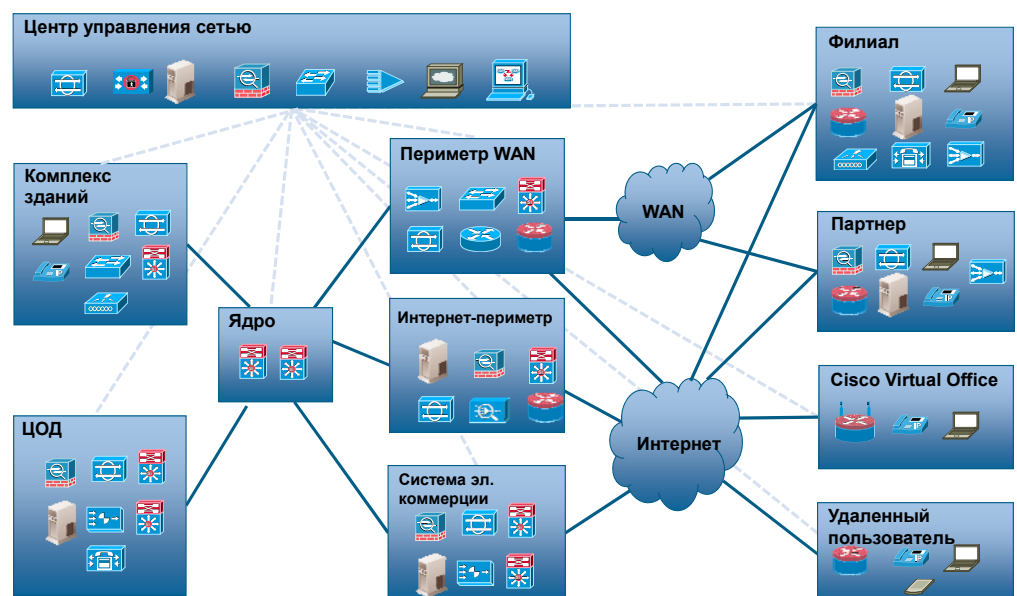
Основные принципы обеспечения безопасности коммутации касаются обеспечения доступности сети коммутации на уровне 2. С этой целью в проектах дизайна предусмотрены следующие функции:

- Ограничение доменов широковещательной рассылки. Разработка инфраструктуры уровня 2, ограничивающей размер доменов широковещательной рассылки.
- Защита протокола STP. Использование имеющихся функций защиты протокола STP.
- Типовые практические рекомендации по организации сетей VLAN

### 5. Дизайны системы безопасности

Дизайн системы безопасности в целом состоит из нескольких взаимосвязанных модулей, каждый из которых представляет функцию или сегмент сети, и которые в совокупности реализуют общую стратегию комплексной защиты. Общий дизайн архитектуры представлен на рисунке 11.

Рисунок 11. Архитектура безопасности Cisco



Каждый модуль тщательно проектируется с целью обеспечить доступность и устойчивость, соответствие нормативным требованиям, гибкость при введении новых сервисов, возможность адаптации к новым требованиям с течением времени и упрощение администрирования<sup>1</sup>.

### 5.1. Принципы разработки дизайна

Далее перечислены основные принципы разработки дизайна.

#### Эшелонированная оборона

Средства обеспечения безопасности новой архитектуры рассредоточены по всей сети согласно концепции эшелонированной обороны и обеспечивают конфиденциальность, целостность и доступность данных, приложений, оконечных устройств и самой сети. Широкий спектр технологий и функций обеспечения безопасности для повышения уровня контроля и управления разворачивается на нескольких уровнях, но в рамках единой стратегии. Выбор технологий и функций определяется концепцией Cisco Security Framework.

#### Доступность и отказоустойчивость сервисов

Проекты архитектуры предусматривают несколько уровней резервирования, что позволяет исключить единственные точки отказа и максимально повысить доступность сетевой инфраструктуры. Кроме того, в проектах используется широкий спектр функций, предназначенных для повышения устойчивости сети к атакам и отказам.

#### Соответствие нормативным требованиям

В архитектуре реализованы встроенные базовые средства обеспечения безопасности, являющиеся существенной частью сетевой инфраструктуры. Базовые средства обеспечения безопасности включают широкий спектр методов и функций обеспечения безопасности, обычно требуемых нормативными документами и стандартами и позволяющих обеспечить соответствие нормативным требованиям.

#### Модульность и гибкость

Дизайн архитектуры выполнен в соответствии с принципами модульности, согласно которым все компоненты описываются функциональными ролями, а не как конкретные точечные решения. Благодаря этому на этапе выбора оптимальной платформы для конкретной функциональной роли повышается гибкость, обеспечивает соответствие сети бизнес-модели компании и развитие ИТ-инфраструктуры вместе с компанией. В то же время модульность проекта способствует внедрению будущих сервисов и ролей, продлевает срок использования имеющегося оборудования и обеспечивает защиту произведенных капитальных вложений.

#### Повышение эффективности эксплуатации

Архитектура ориентирована на обеспечение эксплуатации на протяжении всего жизненного цикла, начиная с развертывания, что способствует снижению эксплуатационных расходов. В дополнении к методическим указаниям по проектированию и начальному развертыванию в данном руководстве представлен перспективный план внедрения, позволяющий пользователям начать с подмножества дизайна и систематически внедрять остальные технологии и функции по мере необходимости. Предусмотрены инструментальные средства и процедуры, ориентированные на эксплуатацию и позволяющие контролировать эффективность и правильность работы каждого элемента сети в проекте.

### 5.2. Сеть комплекса зданий

Сеть комплекса зданий предприятия предоставляет доступ к сети конечным пользователям и устройствам, расположенным на одной территории. Эта сеть может распространяться на несколько этажей в одном здании или несколько зданий, охватывая более обширную территорию. Сеть комплекса зданий может использоваться для предоставления локальных сервисов передачи данных, голоса и видео.

<sup>1</sup> Системы электронной коммерции, Cisco Virtual Office и модули партнеров будут рассмотрены в следующих версиях документа.

### 5.2.1. Направления угроз

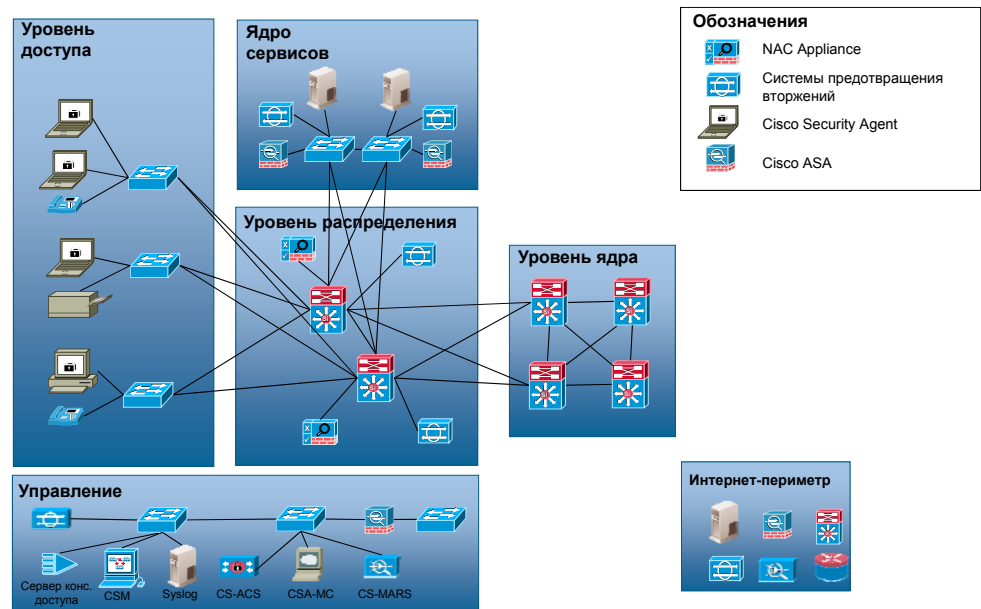
Далее перечислены некоторые направления угроз для сети комплекса зданий.

- Прерывание обслуживания. Ботнеты, вредоносные программы, вирусы, DoS-атаки (переполнение буфера, перегрузка ресурсов конечных устройств), DDoS-атаки на сервисы и инфраструктуру.
- Несанкционированный доступ. Пользователи без надлежащих полномочий, повышение уровня привилегий, несанкционированный доступ к конфиденциальным ресурсам.
- Раскрытие и модификация данных. Прослушивание сетевого трафика, атаки типа "посредник" на данные, передаваемые по сети.
- Злоупотребление сетевыми сервисами. Использование клиентов файлообменных сетей и систем мгновенного обмена сообщениями, просмотр ресурсов, не соответствующих требованиям политики, доступ к запрещенному контенту.
- Утечка данных. Утечка с серверов и пользовательских конечных устройств, утечка хранимых данных и данных, передаваемых по сети.
- Кража персональных данных и мошенничество. Кража персональных данных с серверов и пользовательских конечных устройств, фишинг и спам.

### 5.2.2. Проектирование

В дизайне сети комплекса зданий используется модель трехуровневой сети, в которой выделяются уровень ядра, уровень распределения и уровень доступа. Резервирование достигается за счет внедрения резервируемых коммутаторов и развертывания резервных каналов. Получаемая в результате этого полная топологическая избыточность проиллюстрирована на рис. 12.

Рисунок 12. Топология сети комплекса зданий



В этом дизайне все коммутаторы защищены в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля, защиту динамического обмена маршрутной информацией, а также рекомендуемые методы организации сетей VLAN.

Коммутаторы уровня распределения агрегируют соединения от многочисленных коммутаторов доступа, поэтому их можно использовать в качестве единой точки управления. Система предотвращения вторжений подключается к этим коммутаторам в режиме транзитной передачи трафика с целью идентификации и блокирования

известных атак и подозрительных процессов в сети комплекса зданий. Оповещения и предупреждения, формируемые системой предотвращения вторжений, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей. Коммутаторы уровня распределения также могут реализовывать разделение трафика и разграничение доступа между сетями VLAN. Кроме того, могут быть развернуты функции uRPF, списки ACL и другие механизмы защиты от подмены IP-адресов отправителя.

С целью размещения определенных сервисов для локальных пользователей сети комплекса зданий может быть развернут дополнительный набор сервисных коммутаторов. Межсетевой экран с контролем состояния соединений может использоваться для реализации политики разграничения доступа по отношению к локальным сервисам. К этим сервисным коммутаторам также можно подключить систему предотвращения вторжений. В дополнение система контроля доступа к сети Cisco NAC обеспечивает аутентификацию на основе ролей, проверку состояния безопасности, сетевой карантин и гостевой доступ.

Программное обеспечение защиты конечных устройств защищает настольные и портативные компьютеры, подключенные к коммутаторам доступа. Оповещения и данные мониторинга, формируемые конечными устройствами, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей.

Коммутаторы доступа выполняют функции первой линии защиты от угроз, создаваемых подключенными к ним устройствами. На этом уровне могут быть развернуты функции защиты на уровне портов и протоколов DHCP и ARP. В дополнение, коммутаторы доступа могут поддерживать аутентификацию и доступ на основе ролей для подключенных к ним систем.

В таблице 4 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

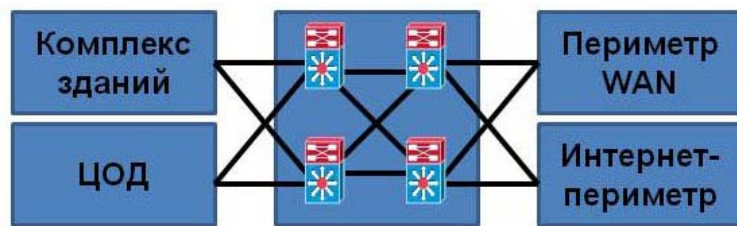
**Таблица 4.** Оценка в соответствии с концепцией CSF. Сеть комплекса зданий

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Аутентификация на уровне локальной сети или порта Глубокий анализ пакетов на межсетевом экране Классификация трафика	Система обнаружения вторжений Сетевое управление Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Защита конечных устройств Резервирование каналов и систем	Сети VLAN Контроль доступа к сети	Разграничение доступа на основе меж сетевого экрана с контролем состояния сеансов Списки ACL, функция uRPF, предотвращение IP-спуфинга Защита на уровне портов Защита инфраструктуры уровня 2 Предотвращение вторжений Применение политики QoS Контроль доступа к сети

#### 5.4. Ядро сети

Ядро сети является элементом инфраструктуры, объединяющим все остальные модули (см. рис. 13). Ядро сети представляет собой высокоскоростную инфраструктуру, предназначенную для предоставления надежных и быстрых сервисов уровня 2 и 3. Ядро сети обычно реализуется на резервированных коммутаторах, которые агрегируют соединения в рамках сетей комплексов зданий, центров обработки данных, граничных сегментов сети для соединения с глобальными сетями и с Интернетом.

Рисунок 13. Топология ядра сети

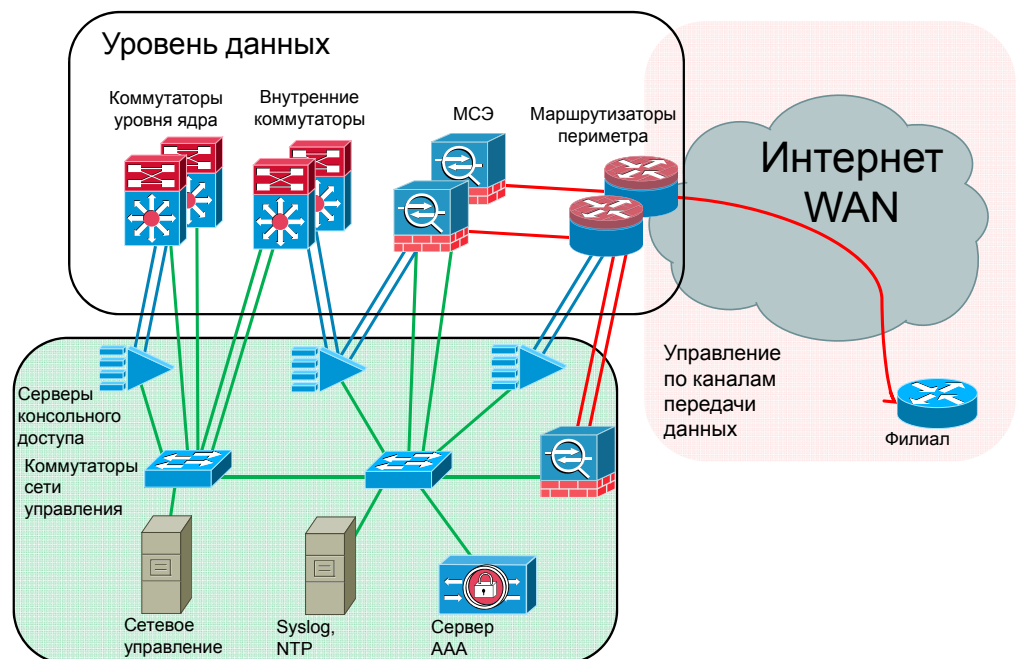


Защита этих коммутаторов ядра сети осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту коммутационной инфраструктуры. Коммутаторы работают в качестве точки объединения потоков сетевого трафика и информации о событиях, используемой для анализа и выявления взаимозависимостей.

#### 5.4. Сеть управления и центр NOC

В дизайн архитектуры включена сеть управления, выполняющая специализированные функции передачи трафика уровней контроля и управления, в частности трафика протоколов NTP, SSH, SNMP, syslog. Сеть управления объединяет механизмы управления по каналам передачи данных и по выделенным каналам (внеполосного и внутриполосного управления) и распространяется на все строительные блоки сети. На рис. 14 показана сеть управления в рамках периметра, подключенного к Интернету.

Рисунок 14. Сеть управления



В центральном офисе компании сеть управления по выделенным каналам реализована на основе выделенных коммутаторов, которые являются независимыми и физически отделены от сети передачи данных. Маршрутизаторы, коммутаторы и другие сетевые устройства подключаются к сети управления по выделенным каналам через выделенные интерфейсы управления. В сети управления по выделенным каналам размещаются серверы консольного доступа, рабочие станции управления сетью, серверы AAA, средства анализа и выявления взаимозависимостей, серверы протоколов NTP, FTP, syslog и все остальные службы управления и контроля. Единая сеть управления по выделенным каналам может обслуживать остальные "функциональные блоки" сети центрального офиса компании.

В случае периметра, подключенного к Интернету, все устройства, находящиеся за межсетевыми экранами периметра, управляются с узлов, расположенных во внутренней области сети, с использованием той же физической и логической инфраструктуры, которая используется для передачи данных. В отличие от устройств, развернутых в центральном офисе компании, внешние коммутаторы и маршрутизаторы периметра размещаются за межсетевым экраном периметра и поэтому управляются по каналам передачи данных. Межсетевые экраны периметра обеспечивают безопасность сети управления по выделенным каналам за счет того, что разрешают соединения для контроля и управления только с разрешенных устройств. Подключение внешних коммутаторов и маршрутизаторов периметра непосредственно к сети управления по выделенным каналам крайне не рекомендуется, поскольку способствует обходу защиты, обеспечиваемой межсетевым экраном. Устройства, находящиеся в филиалах, также должны управляться по каналам передачи данных, но с использованием защищенного VPN-соединения.

По очевидным причинам управление сетями филиалов осуществляется также по каналам передачи данных. В этом случае маршрутизаторы периметра для соединения с глобальными сетями могут обеспечивать подключение к сети управления по выделенным каналам в контролируемом режиме. Доступ должен предоставляться только для явно определенных административных IP-адресов оборудования филиала и только для необходимых протоколов и портов.

### **5.5. Периметр корпоративной сети, подключенный к Интернету**

Периметр сети, подключенный к Интернету – это сетевая инфраструктура, обеспечивающая соединение с Интернетом и выполняющая функции шлюза для ресурсов предприятия при необходимости передачи данных во всемирную сеть.

Периметр, подключенный к Интернету, обслуживает множество других модулей, имеющих в типичной корпоративной сети. Пользователи сети комплекса зданий осуществляют доступ в Интернет через периметр, подключенный к Интернету. Web-сайт организации и другие общедоступные ресурсы доступны клиентам и партнерам через периметр, подключенный к Интернету. Мобильные и работающие дома сотрудники могут получать доступ к корпоративным ресурсам и приложениям через периметр, подключенный к Интернету. Эта инфраструктура может также обеспечивать резервный доступ к удаленным офисам и филиалам в случае отказа основного канала глобальной сети.

Периметр, подключенный к Интернету, обслуживает следующие сценарии использования:

- Демилитаризованная зона (ДМЗ) для общедоступных сервисов. ДМЗ является частью инфраструктуры периметра, подключенного к Интернету, в которой размещаются общедоступные сервисы, доступные из Интернета. Эти сервисы часто включают web-сайт организации, портал для доступа партнеров, сервер электронной почты, FTP-сервер, DNS-сервер и прочие сервисы.
- Корпоративный доступ в Интернет. Инфраструктура периметра, подключенного к Интернету, обеспечивает пользователям, находящимся в центральном офисе или в региональных офисах, доступ в Интернет. Кроме того, эта инфраструктура может обслуживать пользователей, находящихся в филиалах с доступом в Интернет только через централизованное подключение.
- Сети VPN для удаленного доступа. Одной из задач архитектуры периметра, подключенного к Интернету, является обеспечение мобильных пользователей и удаленных работников защищенным доступом к приложениям и данным, находящимся в корпоративной сети.

#### **5.5.1. Направления угроз**

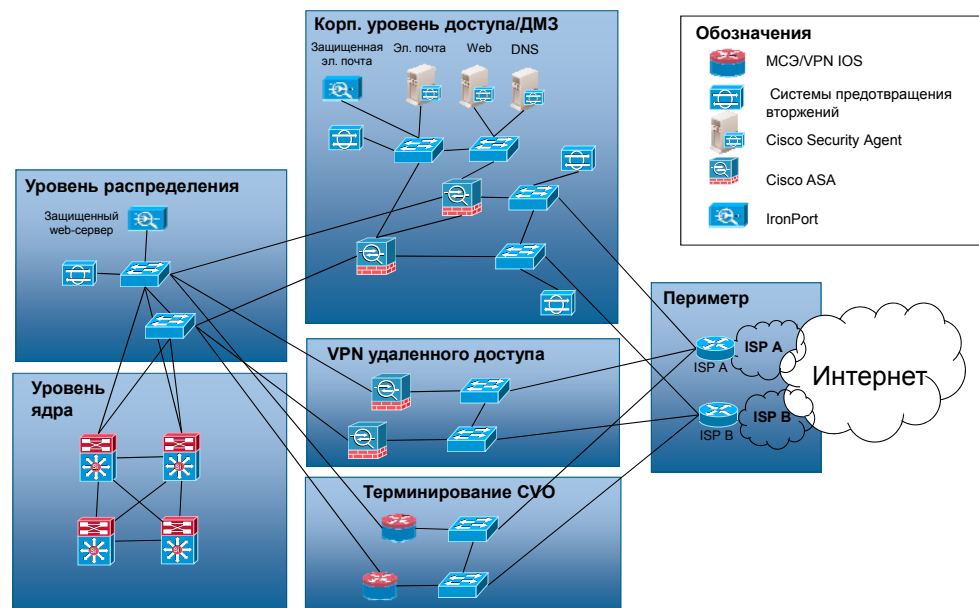
Далее перечислены некоторые направления угроз для сценариев использования, обслуживаемых периметром, подключенным к Интернету.

- Прерывание обслуживания. Ботнеты, специализированные DoS-атаки на серверы (переполнение буфера, использование ресурсов конечных устройств), DDoS-атаки на сервисы и инфраструктуру. Вредоносные программы и заражение вирусами.
- Злоупотребление сетевыми сервисами. Злоупотребление клиентами файлообменных сетей и систем мгновенного обмена сообщениями, просмотр ресурсов, не соответствующих требованиям политики, доступ к запрещенному контенту из сетей комплексов зданий и филиалов, а также через систему удаленного доступа с использованием VPN-соединений.
- Утечка данных. Утечка с серверов и пользовательских конечных устройств, утечка хранимых данных и данных, передаваемых по сети.
- Вторжения и перехват управления. Использование ресурсов общедоступных серверов, несанкционированные модификации web-сайтов.
- Кража персональных данных и мошенничество. Кража персональных данных с серверов и пользовательских конечных устройств, фишинг и спам.

### 5.5.2. Дизайн

Как показано на рис. 15, периметр, подключенный к Интернету, состоит из нескольких функциональных блоков, подключенных к одной или более пар маршрутизаторов периметра. В данной версии документа в периметр входят два блока: блок корпоративного доступа и ДМЗ, а также блок сетей VPN для удаленного доступа.

**Рисунок 15.** Топология периметра, подключенного к Интернету



В данном дизайне основная функция маршрутизаторов периметра заключается в маршрутизации трафика между сетями организации и Интернетом. Они обеспечивают соединение с Интернетом через одного или более Интернет-провайдеров. Маршрутизаторы периметра также могут выполнять функции QoS и ограничения пропускной способности. В терминах безопасности маршрутизаторы периметра выполняют функции первой линии защиты от внешних атак. Для защиты от подмены IP-адресов отправителя и блокирования искаженных пакетов используются списки ACL, функция uRPF и другие механизмы фильтрации. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы netflow, syslog, snmp. Защита маршрутизаторов периметра осуществляется в соответствии с методикой, описанной в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту динамического обмена маршрутной информацией. Резервирование достигается за счет развертывания двух маршрутизаторов и настройки протокола FHRP на их внутренних интерфейсах.

### Блок корпоративного доступа и ДМЗ

Блок корпоративного доступа и ДМЗ обслуживает общедоступные сервисы зоны ДМЗ и обеспечивает доступ в Интернет для пользователей сети комплекса зданий. Блок включает два межсетевых экрана и использует их функции динамического разграничения доступа и глубокого анализа пакетов для следующих целей:

- защита внутренних ресурсов и данных организации от внешних угроз путем запрета входящего доступа из Интернета;
- защита общедоступных ресурсов, размещенных в зоне ДМЗ, путем ограничения входящего доступа к общедоступным сервисам и ограничения исходящего доступа с ресурсов зоны ДМЗ в Интернет;
- контроль пользовательского Интернет-трафика.

Административный доступ к межсетевым экранам также защищен в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". В дизайне реализовано резервирование межсетевых экранов путем использования двух устройств, развернутых в режиме аварийного переключения с сохранением состояния "активное-резервное".

Блок корпоративного доступа и ДМЗ использует пару резервированных внешних коммутаторов, которые обеспечивают соединение на канальном уровне (уровне 2) между маршрутизаторами периметра и межсетевыми экранами. Внешние коммутаторы обеспечивают соединение с компонентом, осуществляющим отражение распределенных атак типа "отказ в обслуживании" (DDoS-атак).

Зона ДМЗ для общедоступных сервисов реализована на основе пары резервированных коммутаторов. Если необходимо развернуть нескольких ферм серверов, они распределяются по различным сетям VLAN, которые объединяются на межсетевых экранах, выполняющих функции контроля трафика между фермами серверов. Все сети VLAN ДМЗ объединяются на межсетевых экранах, и трафик между сетями VLAN не маршрутизируется никакими другими устройствами.

Дизайн также включает пару резервированных внутренних коммутаторов, которые обеспечивают соединение на сетевом уровне (уровне 3) и канальном уровне (уровне 2) между периметром, подключенным к Интернету, и остальной частью корпоративной сети, обычно через ядро сети. На внутренних коммутаторах могут быть настроены процессы маршрутизации, выполняющие маршрутизацию информации между сетями VLAN, которые подключены к коммутаторам ядра сети, и межсетевым экраном внутри сети VLAN.

Защита всех коммутаторов осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту инфраструктуры коммутации.

Необходимо заметить, что функции внутренних и внешних коммутаторов, а также коммутаторов ДМЗ могут быть реализованы в единственной паре коммутаторов. В этом случае внутренний, внешний сегменты и сегмент ДМЗ межсетевого экрана необходимо правильно сегментировать с помощью сетей VLAN.

Сервисы и приложения, размещенные в зоне ДМЗ, защищены межсетевыми экранами периметра с контролем состояния соединений, системой предотвращения вторжений и системой отражения DDoS-атак. Межсетевые экраны периметра защищают зону ДМЗ путем контроля и проверки всего трафика, входящего в сегменты ДМЗ и выходящего из них. Этот трафик включает трафик между зонами ДМЗ, а также трафик между зоной ДМЗ, Интернетом и внутренней сетью. В зоне ДМЗ развернута система предотвращения вторжений, предназначенная для идентификации и блокирования известных атак и подозрительных процессов. Серверы в зоне ДМЗ защищены программным обеспечением защиты оконечных устройств, которое работает совместно с системой предотвращения вторжений и системой мониторинга и анализа. Оповещения и предупреждения, формируемые системой предотвращения вторжений и программным обеспечением защиты оконечных устройств, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей. Кроме того, в зоне ДМЗ

развернута система защиты обмена сообщениями, предназначенная для проверки входящих и исходящих сообщений электронной почты и устранения угроз, например почтового спама, вирусов и червей.

Система обнаружения аномалий развернута во внешнем сегменте. Эта система выполняет функции идентификации DDoS-атак и других сетевых атак и работает совместно с системой отражения DDoS-атак, развернутой на внешних коммутаторах. Когда подтверждается продолжающаяся атака на один из общедоступных сервисов (например, HTTP), система отражения DDoS-атак инициирует перенаправление трафика, чтобы пропускать трафик к сервису, подвергнувшемуся воздействию, через себя, и начинает проверку трафика, гарантируя, что сервера достигает только легитимный трафик.

Межсетевые экраны периметра также выполняют функции реализации политики доступа в Интернет для внутренних пользователей. С этой целью межсетевые экраны реализуют политику доступа, отслеживают состояние соединений и проверяют данные в пакетах. Для выполнения части этих функций межсетевые экраны могут быть настроены на реализацию принципов политики доступа, направленных на ограничение или блокирование мгновенного обмена сообщениями и файлообменных систем для предотвращения злоупотребления сетевыми сервисами.

Система предотвращения вторжений подключается к этим коммутаторам в режиме транзитной передачи трафика для идентификации и блокирования известных атак или вредоносных действий. Система обнаружения вторжений может быть настроена на оповещение о действиях, рассматриваемых как злоупотребление сетевыми сервисами (клиенты файлообменных сетей, системы мгновенного обмена сообщениями и т. д.). Оповещения, формируемые системой предотвращения вторжений, направляются в систему мониторинга и анализа с целью анализа и выявления взаимозависимостей.

Система защиты web-ресурсов развертывается на уровне внутренних коммутаторов для проверки web-трафика, связанного с Интернетом. Эта система выполняет функции блокирования шпионских и вредоносных программ и других известных угроз, а также используется для фильтрации контента и, дополнительно, для аутентификации запросов пользователей.

Обмен сообщениями электронной почты контролируется системой защиты обмена сообщениями, развернутой в ДМЗ, в которой размещается почтовый сервер. Эта система выполняет функции анализа содержимого сообщений электронной почты и устранения угроз, например почтового спама, вирусов и червей.

В таблице 5 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

**Таблица 5.** Оценка в соответствии с концепцией CSF. Доступ в Интернет и ДМЗ

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Глубокий анализ пакетов на межсетевом экране Защита web-ресурсов Фильтрация контента Защита обмена сообщениями	Система обнаружения вторжений Система обнаружения аномалий Сетевое управление Сбор данных о потоках сетевого трафика Сбор пакетов Мониторинг оконечных устройств Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Резервирование каналов и систем	Сети VLAN Защита оконечных устройств	Контроль доступа основе межсетевого экрана с контролем состояния сеансов Предотвращение вторжений Защита оконечных устройств Фильтрация контента Защита обмена сообщениями

### Блок сетей VPN для удаленного доступа

Сети VPN для удаленного доступа обеспечивают защищенные подключения для удаленных пользователей. В блоке реализованы два межсетевых экрана VPN со следующими функциями:

- аутентификация доступа удаленных пользователей;
- поддержка шифрованного доступа к приложениям и данным;
- реализация политики доступа на основе групп или пользователей;
- защита внутренних ресурсов и данных организации от внешних угроз путем проверки уровня протокола и приложения.

Административный доступ к межсетевым экранам защищен в соответствии принципами, описанными в разделе "Подход к защите основы сети SNF". В проекте реализовано резервирование межсетевых экранов путем использования двух устройств, развернутых с поддержкой аварийного переключения в режиме "активное/резервное".

Блок сетей VPN для удаленного доступа включает резервированные внутренние и внешние коммутаторы. Их защита осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту коммутационной инфраструктуры.

Доступ удаленных пользователей требует аутентификации, соответствующий трафик шифруется с использованием средств протоколов SSL или IPSec. VPN-туннели терминируются на группе межсетевых экранов VPN. Межсетевые экраны не только выполняют функции аутентификации пользователей и оконечных точек сеансов VPN, но также реализуют политику доступа на основе пользователей или групп, которая разрешает доступ пользователей только к необходимым ресурсам.

Система предотвращения вторжений, развернутая в режиме транзитной передачи трафика во внутреннем сегменте межсетевого экрана, проверяет трафик, поступающий от удаленных пользователей и отправляемый им. Все оповещения, формируемые системой предотвращения вторжений, направляются в систему мониторинга и анализа с целью анализа и выявления взаимозависимостей.

В том случае, если удаленные пользователи используют централизованный сервис электронной почты, система защиты обмена сообщениями, развернутая вблизи почтового сервера, проверяет весь обмен сообщениями электронной почты, анализирует содержимое сообщений и устраняет угрозы, например почтовый спам, вирусы червей.

Если в соответствии с политикой организации доступ в Интернет осуществляется через центральный офис, web-коммуникации с удаленными пользователями могут также защищаться системой защиты web-ресурсов, развернутой на уровне внутренних коммутаторов.

Кроме того, удаленные пользователи могут быть защищены программным обеспечением защиты оконечных устройств, которое работает совместно с системой предотвращения вторжений и системой мониторинга и анализа. Такая совместная работа обеспечивает более точную оценку уровня риска, связанного с событиями, а также динамическое применение контрольных списков для систем, предположительно подвергшихся угрозе.

В таблице 6 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

**Таблица 6.** Оценка в соответствии с концепцией CSF. Сети VPN для удаленного доступа

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Глубокий анализ пакетов на межсетевом экране Аутентификация VPN Защита web-ресурсов Фильтрация контента* Защита обмена сообщениями*	Система обнаружения вторжений Сетевое управление Защита оконечных устройств Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Резервирование VPN Резервирование каналов и систем	Политика доступа на основе пользователей и групп, реализованная на межсетевом экране Сети VPN	Разграничение доступа на межсетевом экране с контролем состояния соединений Предотвращение вторжений Защита оконечных устройств Фильтрация контента* Защита обмена сообщениями*

\* Для случая, когда доступ в Интернет разрешен только через центральный офис.

### 5.6. Периметр, подключенный к глобальной сети

Периметр, подключенный к глобальной сети, является элементом сетевой инфраструктуры, который агрегирует каналы глобальной сети, соединяющие географически удаленные филиалы с центральным офисом или региональным узловым офисом. Канал подключения к глобальной сети может находиться в собственности предприятия или предоставляться провайдером услуг, что встречается чаще. Задача глобальной сети состоит в том, чтобы предоставить пользователям, находящимся в филиалах, такие же сетевые сервисы, что и пользователям, находящимся в центральном офисе.

Периметр, подключенный к глобальной сети, также поддерживает защищенные соединения по глобальной сети с использованием сетей VPN уровня 2 или 3, часто предлагаемых провайдером услуг.

#### 5.6.1. Направления угроз

Далее перечислены некоторые направления угроз в отношении граничного сегмента для соединения с глобальной сетью.

- Прерывание обслуживания. Ботнеты, вредоносные программы, вирусы. DDoS-атаки, направленные на сервисы и инфраструктуру.
- Раскрытие и изменение данных. Подмена IP-адресов отправителя, атаки типа "посредник" на данные, передаваемые по сети.
- Злоупотребление сетевыми сервисами. Злоупотребление клиентами файлообменных сетей и систем мгновенного обмена сообщениями, просмотр ресурсов, не соответствующих требованиям политики, доступ к запрещенному контенту из филиалов.

#### 5.6.2. Дизайн

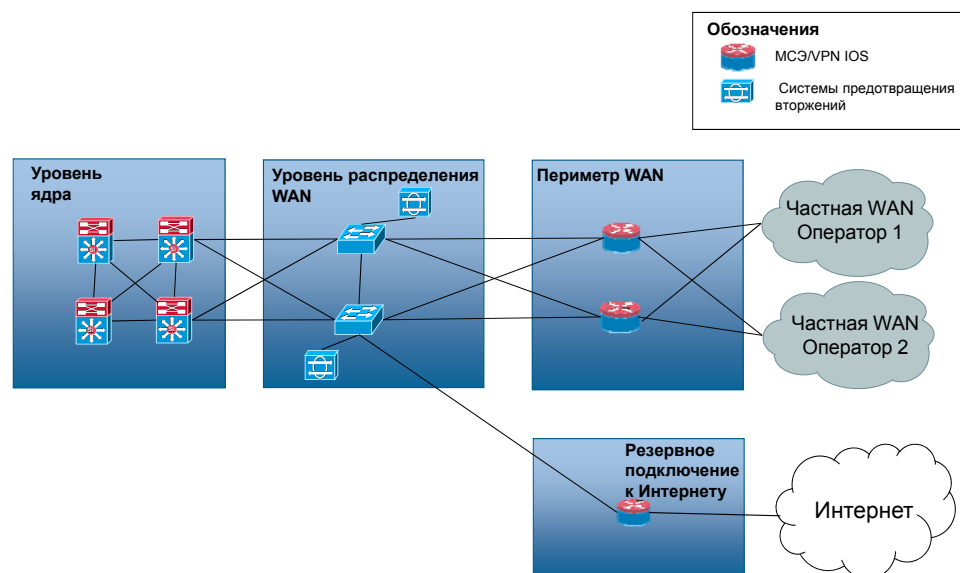
В данном проекте рассматриваются следующие ключевые задачи безопасности:

- Повышение уровня защищенности сетевой инфраструктуры.
- Повышение уровня защищенности каждого устройства, входящего в сетевую инфраструктуру, защита сервисов маршрутизации и коммутации, реализация основных принципов сетевой политики.
- Защищенные коммуникации.
- Шифрование трафика, передаваемого по глобальной сети.

- Обнаружение и отражение угроз.  
Использование различных видов сетевой телеметрии и интеграция системы предотвращения вторжений в головной сегмент корпоративной сети.
- Мониторинг сети.  
Поддержка основных операций по обеспечению безопасности за счет внедрения сетевой телеметрии и инструментальных средств обнаружения аномалий и выявления взаимозависимостей.

Как показано на рис. 16, дизайн периметра, подключенного к глобальной сети, реализован на паре резервированных маршрутизаторов с поддержкой подключения к глобальной сети. Эти маршрутизаторы агрегируют каналы, идущие к филиалам и другим региональным офисам. Защита маршрутизаторов периметра осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Эти маршрутизаторы также могут выполнять функции QoS и ограничения пропускной способности. Чтобы разрешить только трафик, поступающий из доверенных источников, могут применяться списки ACL. Для защиты от подмены IP-адресов отправителя и блокирования искаженных пакетов используются списки ACL, функция uRPF и другие механизмы фильтрации. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы netflow, syslog, snmp.

**Рисунок 16.** Топология граничного сегмента для соединения с глобальной сетью



Пара маршрутизаторов VPN развертывается за маршрутизаторами уровня агрегирования. Они выполняют функции аутентификации конечных устройств VPN и конечных точек шифрованных туннелей. В данном дизайне для упрощения настройки используются сети VPN с динамической групповой адресацией (Dynamic Multicast VPN, DMVPN). Защита маршрутизаторов VPN также осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Маршрутизаторы могут также поддерживать функции QoS и ограничения пропускной способности. Маршрутизаторы могут выполнять контроль трафика между сетями VPN через центральное устройство с использованием списков ACL. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы netflow, syslog, snmp.

Пара резервированных коммутаторов уровня распределения соединяет маршрутизаторы VPN с ядром сети. Система предотвращения вторжений подключается к этим коммутаторам в режиме транзитной передачи трафика с целью идентификации и блокирования известных атак и подозрительных процессов, связанных с сетями филиалов. Оповещения и предупреждения, формируемые системой предотвращения вторжений, обрабатываются системой мониторинга и анализа с целью анализа и

выявления взаимозависимостей. Защита этих коммутаторов осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF".

В дизайне также предусмотрено дополнительное резервное соединение через Интернет на случай отказа основного соединения через глобальную сеть. Резервное соединение через Интернет реализовано на основе отдельного набора маршрутизаторов VPN, выделенных для аутентификации филиалов, выполнения функций конечной точки зашифрованных туннелей и применения политики межсетевого экрана. Маршрутизаторы, осуществляющие резервное соединение через Интернет, подключаются к маршрутизаторам периметра, подключенного к Интернету, которые настраиваются в соответствии с рекомендациями, представленными в разделе "Периметр, подключенный к Интернету". Согласно этой настройке в случае отказа канала глобальной сети для соединения с филиалом трафик автоматически перенаправляется через Интернет по аутентифицированному и зашифрованному VPN-каналу. VPN-канал может быть либо постоянным, либо устанавливаться по запросу после обнаружения отказа. В данном проекте для идентификации отказов и перенаправления трафика через VPN-туннели используется протокол динамической маршрутизации. Данные протокола динамической маршрутизации передаются как по основным каналам глобальной сети, так и по VPN-туннелям. Эти маршрутизаторы могут применять политики межсетевого экрана с контролем состояния соединений для контроля трафика, поступающего из филиалов или направляемого в них.

Защита маршрутизаторов для резервного соединения через Интернет осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Для защиты от подмены IP-адресов отправителя и блокирования искаженных пакетов могут быть дополнительно настроены списки ACL, функция uRPF и другие механизмы фильтрации. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы netflow, syslog, snmp.

В таблице 7 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

**Таблица 7.** Оценка в соответствии с концепцией CSF. Периметр, подключенный к глобальной сети и Интернету

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Аутентификация VPN Глубокий анализ пакетов на межсетевом экране Классификация трафика	Система обнаружения вторжений Сетевое управление Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Резервирование VPN Резервирование каналов и систем	Сети VPN Сети VLAN	Разграничение доступа на межсетевом экране с контролем состояния событий ACL-списки, функция uRPF, предотвращение IP-спуфинга Предотвращение вторжений Применение политики QoS

## 5.7. Филиал

Сети филиалов обеспечивают возможность подключения пользователей и устройств, находящихся на территории филиала. Обычно они состоят из одной или нескольких локальных сетей и соединяются с центральным узлом через частную глобальную сеть или соединение с Интернетом. Сети филиалов могут использоваться для предоставления локальных сервисов передачи данных, голоса и видео.

### 5.7.1. Направления угроз

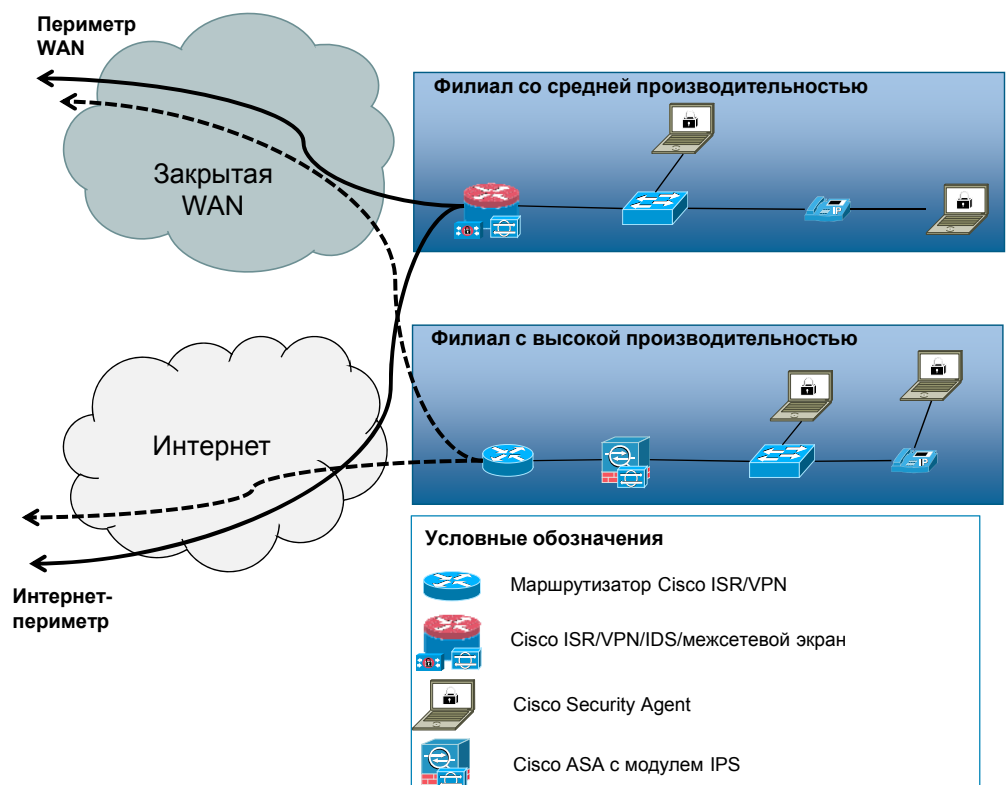
Далее перечислены некоторые направления угроз в отношении периметра, подключенного к глобальной сети.

- Прерывание обслуживания. Ботнеты, вредоносные программы, вирусы, DDoS-атаки, направленные на сервисы и инфраструктуру.
- Несанкционированный доступ. Пользователи без полномочий, повышение уровня привилегий, несанкционированный доступ к конфиденциальным ресурсам.
- Раскрытие и изменение данных. Подмена IP-адресов отправителя, атаки типа "человек посередине" на данные, передаваемые по сети.
- Злоупотребление сетевыми сервисами. Злоупотребление клиентами файлообменных сетей и систем мгновенного обмена сообщениями, просмотр ресурсов, не соответствующих требованиям политики, доступ к запрещенному контенту из филиалов.

### 5.7.2. Дизайн

В данную версию архитектуры включены два дизайна сети филиала. Один из них – сеть филиала типичного размера с умеренной скоростью соединения по глобальной сети и сервисами, интегрированными в маршрутизатор. Другой проект – сеть филиала с более высокими характеристиками, оборудованная устройствами защиты, с более высокой пропускной способностью подключения к глобальной сети. Оба проекта показаны на следующем рисунке.

Рисунок 17. Топологии сети филиала.



#### Сеть филиала со средними характеристиками

В этом проекте предполагается наличие подключения к глобальной сети со средней пропускной способностью до 1,5 Мбит/с. В сети используется маршрутизатор с интеграцией сервисов, в частности, межсетевым экраном, системой предотвращения вторжений и средствами организации сетей VPN. Маршрутизатор также может предоставлять сервис IP-ATC Call Manager Express. Его защита осуществляется в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF". Для защиты от подмены IP-адресов отправителя и блокирования искаженных пакетов используются списки ACL, функция uRPF и другие механизмы фильтрации. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы syslog, snmp.

Коммутатор уровня 2 обеспечивает подключение портов к оконечным устройствам и другим узлам. Его защита осуществляется в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту DHCP, ARP и других жизненно важных протоколов.

Защита оконечных устройств осуществляется с использованием специализированного программного обеспечения. Оповещения и предупреждения, формируемые системой предотвращения вторжений и программным обеспечением защиты оконечных устройств, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей.

#### Сеть филиала с высокими характеристиками

В этом проекте предполагается наличие подключения к глобальной сети с высокой пропускной способностью (не менее 40 Мбит/с). Маршрутизатор в основном используется для маршрутизации и организации сетей VPN и, кроме того, может предоставлять сервисы передачи голоса, например IP-ATC Call Manager Express. Защита этого маршрутизатора осуществляется в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF". Для защиты от подмены IP-адресов отправителя (спуфинга) и блокирования искаженных пакетов используются списки ACL, функция uRPF и другие механизмы фильтрации. Для контроля потоков трафика, сетевых операций и состояния систем используются протоколы syslog, snmp.

Межсетевой экран и система предотвращения вторжений реализованы на основе интегрированного устройства защиты. Административный доступ к межсетевым экранам должен быть защищен в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF".

Коммутатор уровня 2 обеспечивает подключение портов к оконечным устройствам и другим узлам. Его защита осуществляется в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF". Меры защиты включают ограничение и контроль административного доступа, защиту уровней управления и контроля и защиту DHCP, ARP и других жизненно важных протоколов.

Защита оконечных устройств осуществляется с использованием специализированного программного обеспечения. Оповещения и предупреждения, формируемые системой предотвращения вторжений, размещенной на устройстве защиты, и программным обеспечением защиты оконечных устройств, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей.

В таблице 8 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

**Таблица 8.** Оценка в соответствии с концепцией CSF. Сеть филиала

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Аутентификация VPN Глубокий анализ пакетов на межсетевом экране Классификация трафика	Система обнаружения вторжений Сетевое управление Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Защита оконечных устройств Резервирование VPN Резервирование каналов и систем	Сети VPN Сети VLAN	Разграничение доступа на межсетевом экране с контролем состояния соединений Списки ACL, функция uRPF, предотвращение IP-спуфинга Защита на уровне портов Защита инфраструктуры уровня 2 Предотвращение вторжений Применение политики QoS

## 5.8. Центр обработки данных в сети интранет

Сети центров обработки данных в интранете предназначены для размещения систем, которые обслуживают приложения и осуществляют хранение данных, доступных только для внутренних пользователей. Поддерживающая их инфраструктура обычно включает серверы приложений, системы хранения данных, маршрутизаторы, коммутаторы, средства распределения нагрузки, средства разгрузки, устройства для ускорения работы приложений и другие системы. Поскольку доступ к центрам обработки данных в интранете осуществляется из внутренней сети, они проектируются для обеспечения минимальных задержек и максимальной пропускной способности.

### 5.8.1. Направления угроз

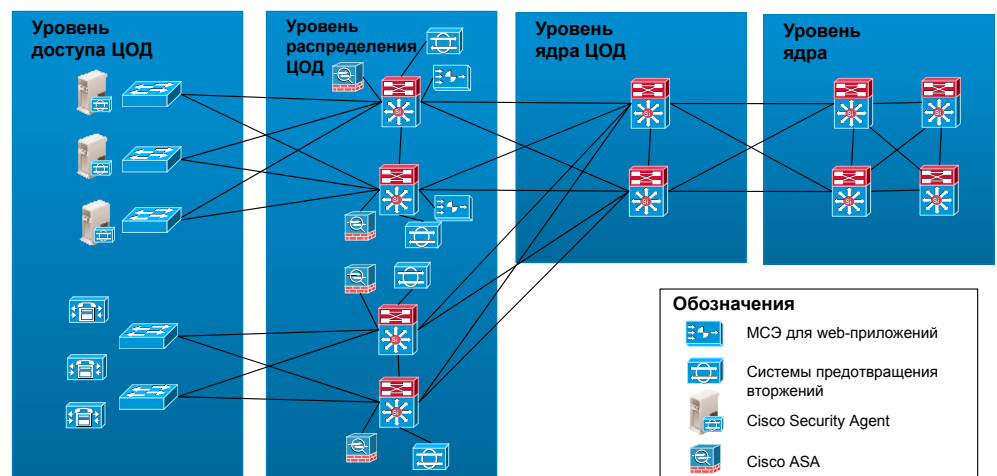
Далее перечислены некоторые направления угроз для сети центра обработки данных в интранете.

- Прерывание обслуживания. Ботнеты, специализированные DoS-атаки на серверы (переполнение буфера, использование ресурсов конечных устройств), DDoS-атаки на сервисы и инфраструктуру.
- Утечка данных. Утечка с серверов хранимых данных и данных, передаваемых по сети.
- Нарушение конфиденциальности и целостности данных, хранящихся в системе и передаваемых по сети.
- Вторжения и перехват управления. Использование ресурсов общедоступных серверов, несанкционированные модификации web-сайтов.
- Кража персональных данных и мошенничество. Кража персональных данных с серверов и пользовательских конечных устройств, фишинг и спам в электронной почте.

### 5.8.3. Дизайн

Проект сети центра обработки данных в интранете следует иерархической модели, состоящей из ядра, уровня распределения и уровня доступа. Пара коммутаторов уровня 2 и 3 образуют ядро сети центра обработки данных, которое агрегирует каналы от других центров обработки данных. Этот элемент инфраструктуры имеет смысл в сетях с несколькими центрами обработки данных. Защита этих коммутаторов осуществляется в соответствии с рекомендациями, описанными в разделе "Подход к защите основы сети SNF".

Рисунок 18. Топология сети центра обработки данных в сети интранет



В проекте архитектуры предусмотрено два резервированных коммутатора уровня распределения, выполняющих агрегирование каналов уровня 2 и 3, по которым подключаются коммутаторы доступа. Если необходим многоуровневый проект, каждый уровень реализуется как отдельная сеть VLAN, которая может распространяться от уровня распределения до коммутаторов доступа.

В проекте используются межсетевые экраны с контролем состояния соединений, настроенные в режиме аварийного переключения при отказе для защиты серверов и обеспечения соответствующего разделения между уровнями приложений. Кроме того, функция гибкого анализа пакетов, реализованная на межсетевом экране, используется для отражения DoS-атак и нормализации трафика. Защита web-приложений усовершенствована за счет использования меж сетевого экрана web-приложений.

Кроме того, используется система обнаружения вторжений, предназначенная для идентификации и блокирования известных атак и подозрительных процессов. В дополнение к системе обнаружения вторжений на web-уровне развернута система обнаружения аномалий. Эта система выполняет функции идентификации DDoS-атак и других сетевых атак и работает совместно с системой отражения DDoS-атак, развернутой за межсетевыми экранами. Когда подтверждается продолжающаяся атака на один из общедоступных сервисов (например, HTTP), система отражения DDoS-атак выполняет перенаправление трафика, чтобы обеспечить транзитную передачу трафика к сервису, подвергнувшемуся воздействию, через себя и начинает проверку трафика, гарантируя, что сервера достигает только легитимный трафик.

Серверы, расположенные на разных уровнях, защищены программным обеспечением защиты оконечных устройств. Оповещения и предупреждения, формируемые системой обнаружения вторжений и программным обеспечением защиты оконечных устройств, обрабатываются системой мониторинга и анализа с целью анализа и выявления взаимозависимостей.

Защита этих коммутаторов осуществляется в соответствии с принципами, описанными в разделе "Подход к защите основы сети SNF". Кроме того, на коммутаторах доступа может быть настроена защита на уровне портов и другие функции защиты уровня 2.

В таблице 9 показано, как все эти компоненты работают совместно в рамках единой стратегии безопасности.

**Таблица 9.** Оценка в соответствии с концепцией CSF. Сеть ЦОД в сети интранет

Общий контроль		
Идентификация	Отслеживание	Выявление взаимозависимостей
Глубокий анализ пакетов на межсетевом экране Цифровые сертификаты.	Система обнаружения вторжений Система обнаружения аномалий Сетевое управление Сбор данных о потоках сетевого трафика Захват пакетов Мониторинг оконечных устройств Отслеживание событий	Анализ и выявление взаимозависимостей событий
Общее управление		
Повышение уровня защищенности	Изоляция	Обеспечение выполнения политики
Базовые средства защиты сети Защита оконечных устройств Резервирование каналов и систем	Сети VLAN Политика разграничения доступа на межсетевом экране Снижение вычислительной нагрузки, связанной с SSL	Разграничение доступа на межсетевом экране с контролем состояния соединений Предотвращение вторжений Защита оконечных устройств Фильтрация контента Защита уровня 2 (CISF)

## 6. Услуги Cisco в сфере информационной безопасности

Архитектура системы безопасности дополняется богатым портфелем услуг Cisco в области информационной безопасности, предназначенных для поддержки решения в течение всего жизненного цикла. Средства безопасности интегрированы во все элементы сетевой инфраструктуры, и благодаря концепции услуг, предоставляемых в течение всего жизненного цикла, предприятия могут развертывать, эксплуатировать и оптимизировать сетевые платформы, которые защищают критически важные бизнес-процессы от атак и прерывания работы, гарантируют защиту конфиденциальности и поддерживают средства контроля соответствия политике и нормативным требованиям.

На следующем рисунке концепция услуг Cisco в области информационной безопасности в течение всего жизненного цикла решения.

**Рисунок 19.** Услуги Cisco в сфере информационной безопасности в течение всего жизненного цикла решения



#### Стратегия и оценки

Cisco предлагает всеобъемлющий комплекс услуг по оценке, основанных на структурированном подходе к консультациям в сфере оптимизация ИТ-решений, управления рисками и соответствия нормативным требованиям в области информационной безопасности. Эти услуги помогают заказчикам понять потребности своих организаций и выявить недостатки, представляют рекомендации по исправлению недочетов на основе отраслевых и международных передовых методик. Они позволяют заказчикам осуществлять стратегическое планирование развития программы информационной безопасности, включая обновление политики безопасности, процессов и технологий.

#### Развертывание и миграция

Cisco предлагает услуги развертывания для поддержки заказчиков на этапах планирования, проектирования и внедрения продуктов и решений компании Cisco для обеспечения информационной безопасности. В дополнение к этому, Cisco предлагает услуги поддержки заказчиков по совершенствованию политики безопасности и процессов, основанные на средствах контроля, которые повышают эффективность работы персонала и архитектуры системы безопасности.

#### Удаленное управление

Технические специалисты службы удаленного управления Cisco Remote Management Services дополняют штат ИТ-подразделений заказчиков, ежедневно и круглосуточно осуществляя профилактический мониторинг технологической инфраструктуры системы безопасности и обеспечивая управление инцидентами, проблемами, изменениями, настройкой и обновлениями, а также управленческую отчетность.

#### Аналитика в области информационной безопасности

Услуги Cisco Security Intelligence обеспечивают ранний сбор информации, анализ и проверенные технологии отражения угроз, помогая специалистам по безопасности реагировать на новые виды угроз. Персонал ИТ-подразделения заказчика может использовать оповещения о новых видах угроз, анализ уязвимости и прикладные технологии отражения угроз, разработанные специалистами Cisco, которые используют глубокие знания и сложные инструментальные средства для проверки аномалий и

разработки технологий, обеспечивающих своевременное, точное и быстрое разрешение проблем, связанных с потенциальной уязвимостью и атаками.

#### **Оптимизация системы безопасности**

Услуга по оптимизации системы безопасности Cisco представляет собой интегрированные услуги, предназначенные для оценки, разработки и оптимизации инфраструктуры системы безопасности заказчиков на постоянной основе. Проводя ежеквартальные посещения объектов заказчика и постоянно выполняя анализ и настройку, группа специалистов Cisco по безопасности дополняет штат ИТ-специалистов заказчика по безопасности и осуществляет их поддержку в обеспечении безопасности бизнеса и управлении рисками на долговременной основе, а также предлагает краткосрочные тактические решения для устранения растущих угроз безопасности.

#### **7. Ссылки**

Network Security Baseline

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline\\_Security/securebasebook.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html)

Архитектура Enterprise Campus 3.0: обзор и структура

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html>



Cisco  
Россия, 115054, Москва,  
бизнес-центр «Риверсайд Тауерс»,  
Космодамианская наб., 52, стр. 1, 4-й этаж.  
Телефон: +7 (495) 961 1410  
Факс: +7 (495) 961 1469  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Россия, 191186, Санкт-Петербург,  
бизнес-центр «Регус»,  
Невский пр-т, 25, 2-й этаж, офисы 9, 30.  
Телефон: +7 (812) 336 6531  
Факс: +7 (812) 346 7800  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco  
Россия, 630099, Новосибирск,  
бизнес-центр «Росевроплаза»,  
Димитрова пр-т, 2, 5-й этаж.  
Телефон: +7 (383) 230 2670  
Факс: +7 (383) 230 1795  
[www.cisco.ru](http://www.cisco.ru)  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco Logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)