DOI 10.37882/2223-2966.2024.01.11

МЕТОДЫ СНИЖЕНИЯ ВОЗНИКНОВЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ SDN

METHODS OF MITIGATING INFORMATION SECURITY RISKS IN SDN NETWORKS

Wang Xinyu

Summary. The article discusses issues related to the consideration of methods of information security risks in SDN networks. The concept of the definition of «SDN network» is considered. The main components of this network have been studied. A comparative characteristic of the difference between the parameters of the traditional network and the SDN network is carried out. The author of the article emphasizes the advantages of using the SDN network to solve simple and complex tasks in practice. The definition of the concept of «risk» is considered. It is noted that the methods of assessing information security risks are divided into qualitative and quantitative. The main methods of reducing the occurrence of risks are considered. General recommendations for reducing information security risks in SDN networks have been developed.

Keywords: methods, risks, occurrence, information security, SDN networks, reduction.

Ван Синьюй
Шеньянский университет аэронавтики и астронавтики, Шеньян, Китай
1179384407@qq.com

Аннотация. В статье рассматриваются вопросы, связанные с рассмотрением методов возникновения рисков информационной безопасности в сетях SDN. Рассмотрено понятие определения «сеть SDN». Изучены основные компоненты данной сети. Проведена сравнительная характеристика отличия параметров традиционной сети от сети SDN. Автор статьи подчеркивает преимущества использования сети SDN для решения простых и сложных задач на практике. Рассмотрено определение понятия «риск». Отмечено, что методы оценки рисков информационной безопасности делятся на качественные и количественные. Рассмотрены основные методы снижения возникновения рисков. Разработаны общие рекомендации по снижение рисков информационной безопасности в сетях SDN.

Ключевые слова: методы, риски, возникновение, информационная безопасность, сети SDN, снижение.

Введение

Проблемы обеспечения информационной безопасности на предприятиях и организациях играют ключевую роль в обеспечении стабильности их работы, дальнейшего развития и процветания. Поскольку всевозможные риски и угрозы мешают деятельности хозяйствующих субъектов рынка, снижают прибыль, рентабельность и эффективность работы в целом. Особенно неблагоприятное воздействие на функционирование предприятий и организаций оказывают риски информационной безопасности. Следовательно, на данном этапе очень важно уделить большое внимание оценке и прогнозированию данному виду рисков.

Основные результаты

Сеть SDN представляет собой непрерывный поток передачи данных путем с помощью программного обеспечения путем удаленного доступа. Данная сеть включает в себя различные компоненты, к которым можно отнести:

1. уровень приложений — включает в себя наличие приложений, которые направлены на расширение возможностей сетевых услуг;
2. уровень плоскости управления — представляет собой центр управления данной системой, осуществляет непосредственный контроль, принимает запросы, поступающие в приложения, а также ведет их обработку;
3. уровень инфраструктуры — определяется наличием и возможностями использования программного оборудования, к которому относятся сетевое оборудование, маршрутизаторы, коммутаторы и т.д.

На Рисунке 1 наглядным образом представлены основные компоненты сети DNS.

Существует различные типы сетей SDN, имеющие определенный функционал и назначение. Так, существует открытая сеть, сеть с интерфейсами, гибридная сеть и другие. Каждая сеть имеет свое назначение, параметры управления, программы и протоколы [1, с. 78].

Прежде чем приступить к рассмотрению методов возникновения рисков информационной безопасности в сетях SDN, считаем необходимым рассмотреть особенности самой сети и чем она отличается от традиционных сетей. Во-первых, традиционная сеть имеет сетевую структуру, которая собирает информацию для последующего выполнения алгоритма маршрутизации. Во-вторых, в случае сбоя она имеет автоматическое схождение. Но в целом данная сеть имеет высокую степень надежности и широкого применения. Что касается

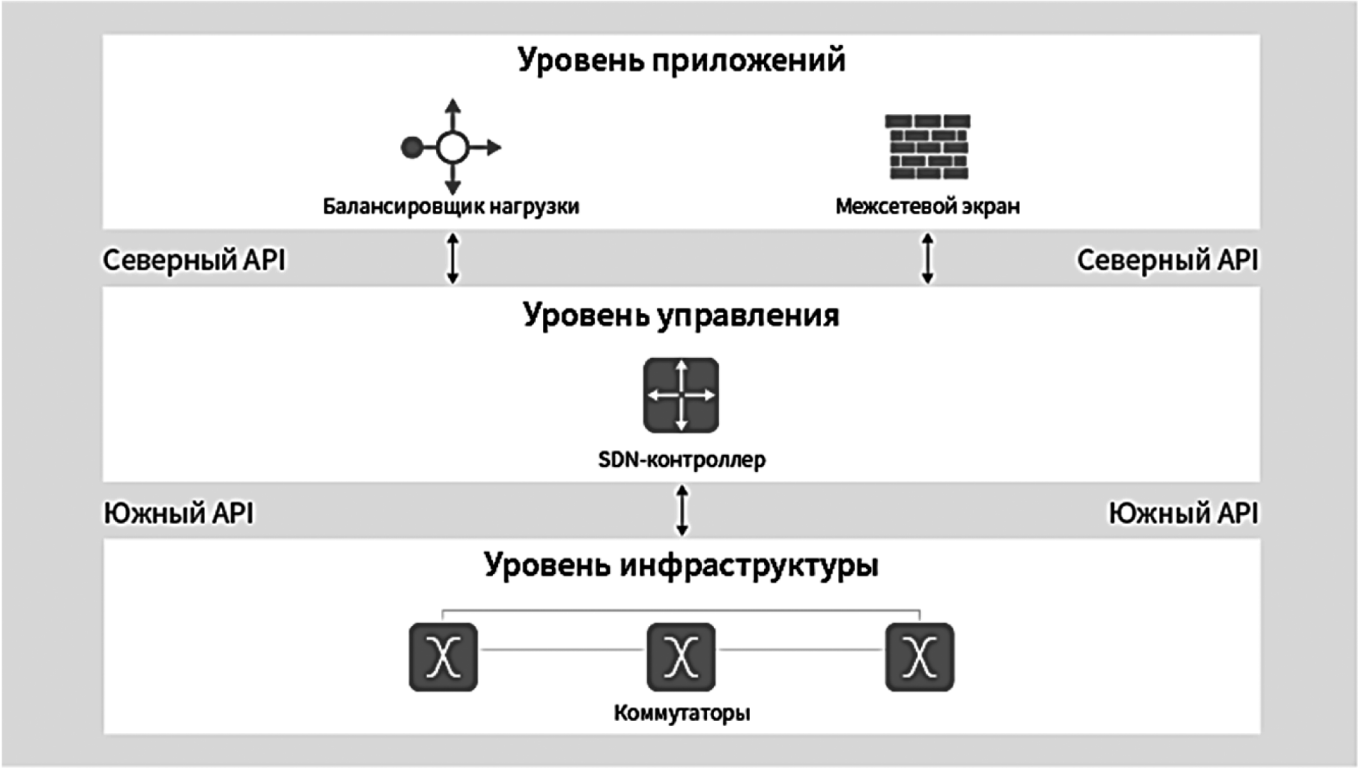

Рис. 1. Основные компоненты сети SDN

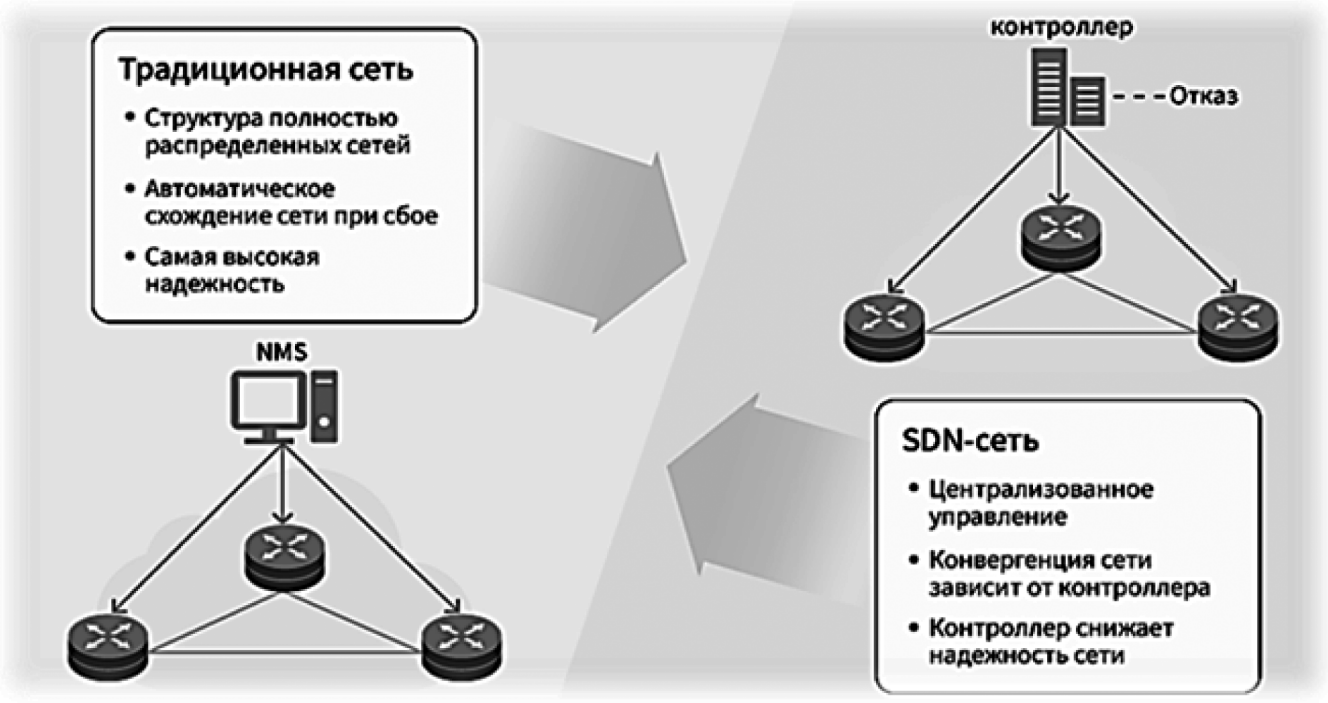

Рис. 2. Отличительные характеристики традиционной сети от сети SDN

сети SDN, то она имеет централизованное управление. Конвергенция сети зависит непосредственно от контролера, который отвечает за параметры надежности сети. На Рисунке 2 представлены основные отличия традиционной сети от сети SDN.

В целом можно отметить, что сеть SDN обладает более широкими возможностями управления, гибкостью системы и ее скоростью совершения операций. Система также характеризуется широким функционалом программного оборудования и управлять большим потоком

данным в реальном режиме времени. Кроме того, сеть SDN имеет разветвленную инфраструктуру, что позволяет администраторам оптимизировать процесс работы и преобразование данных в сети. И наконец, самое главное преимущество использования данной системы заключается в ее высоком уровне безопасности, что позволяет снизить риски и угрозы возникновения потерь, утечки информации, кражи и хищений [4, с.3].

Далее рассмотрим основные методы возникновения рисков информационной безопасности в сетях SDN. Под риском следует понимать вероятность возникновения того или иного события, которое может повлечь за собой неблагоприятные последствия (потери) в будущем.

В целом стоит отметить, что все методы оценки рисков информационной безопасности делятся на две группы: качественные и количественные. Количественные методы основаны на расчете количественных показателей в абсолютном и относительном выражении. При количественном подходе каждому конкретному виду риска присваивается значение или ранг. Далее рассчитывается вероятность наступления того или иного риска с количественным прогнозированием возможного ущерба.

Качественные методы основаны на присвоении риску бальной оценки (степени) экспертным путем. Вначале определяется система ценностей и выстраивается шкала. Далее рассчитывается вероятность наступления угрозы риска и присваивается соответствующая степень оцениваемой угрозы (то есть выставляется оценка). Проводится детальный анализ и разрабатываются конкретные защитные меры для каждого риска.

Одним из самых распространенных методов определения рисков является метод под названием OpenFlow, который направлен на выявление возможных несоответствий в данной сети путем проведения верификации. Популярность обращения у данному методу для оценки и прогнозирования рисков заключается в удобстве и простоте его использования. Основными компонентами системы является коммутатор, контроллер, сетевая операционная система и приложения. На коммутатор поступает большой объем информации, которую он передает контролеру. Контроллер в свою очередь обрабатывает данную информацию, при этом он расходует время и память. В процессе обработки выявляются факторы риска и угрозы информационной безопасности. Коммутатор принимает команды от контроллера и тревожные сигналы для принятия дальнейших решений и действий [3, с.126].

Другим современным методом обеспечения информационной безопасности в сетях SDN является использование методики определения актуальных угроз под названием STRIDE. Рассматриваемая методика включается в себя последовательную оценку рисков по следующим основным параметрам и характеристикам угроз, представленным в Таблице 1.

Таблица 1.

Основные параметры угроз в методологии STRIDE

Угроза	Описание
Спуфинг	Позволяет злоумышленникам скрыть или подделать их личность. Данный тип атак становится возможным ввиду отсутствия надлежащей аутентификации.
Модификация	Позволяет злоумышленникам поставить под угрозу целостность передаваемых или хранимых данных.
Отказ от авторства	Позволяет пользователям в системе отречься от своих действий или обвинить в них других. Системы мониторинга и журналы действий при этом не способны корректно идентифицировать злоумышленника.
Разглашение информации	Эксплуатация этой уязвимости может привести к раскрытию значимой информации или паролей. Она также часто коррелирует с атаками подмены и модификации.
Отказ в обслуживании	Устройства могут подвергаться атаке, которая делает службу или систему временно непригодными для клиентов или пользователей. Этот метод оказывает значительное финансовое влияние и поэтому является одной из наиболее распространенных угроз.
Повышение привилегий	Эта уязвимость часто возникает из-за отсутствия контроля доступа. Простой пользователь или клиент может повысить свои полномочия в системе, что дает им возможность свободного доступа к ограниченным или классифицированным активам.

Таким образом, на основе тщательного анализа параметров угроз определяются средства и инструменты обеспечения информационной безопасности [5, с.10].

Оригинальное решение, позволяющее защитить все серверы, а не только периметр и сегменты сети, было реализовано при интеграции FortiGate-VMX с платформой VMware NSX. В классических ЦОДах злоумышленник может выбрать в качестве цели один из «забытых» низкоприоритетных серверов. Если ему удается проникнуть за защиту периметра и перехватить управление сервером, он длительное время может относительно свободно чувствовать себя внутри периметра и собирать информацию. Благодаря же связке технологии VMware NSX и решения FortiGate-VMX такая возможность для него закрывается, причем без значительного возрастания нагрузки на вычислительные мощности.

Также решения Fortigate обеспечивают дополнительную безопасность Cisco Application Centric Infrastructure (ACI) в условиях ориентированной на приложения инфраструктуры. Cisco ACI приобрело популярность в модели оказания облачных сервисов, делая их более

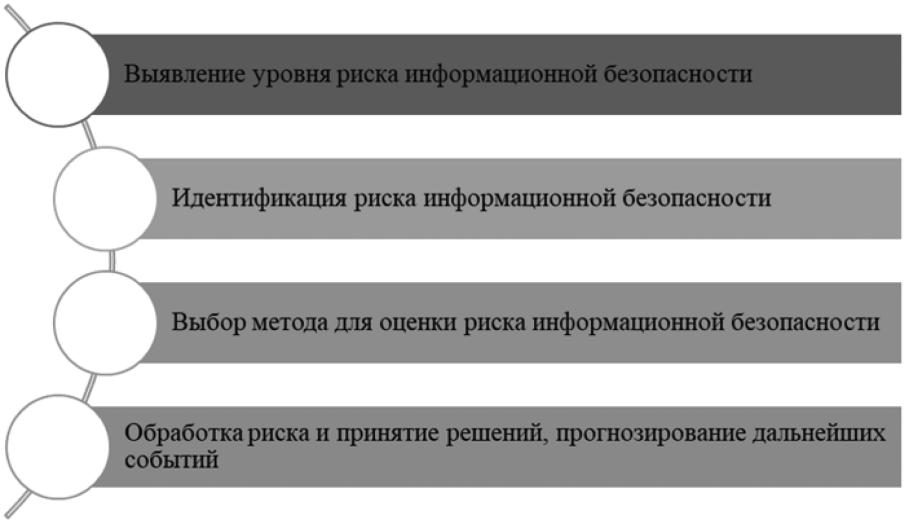

Рис. 3. Рекомендации по снижение рисков информационной безопасности в сетях SDN [Разработано автором]

гибкими. Традиционно вычислительные сети и сетевая безопасность жестко привязаны к оборудованию, что делает сложной настройку и повышает операционные расходы. Совместное решение Fortigate и Cisco позволяет автоматизировать обновления политик и повысить прозрачность безопасности.

В данной статье разработаны общие рекомендации по снижению рисков информационной безопасности в сетях SDN, которые представлены на Рисунке 3.

Считаем, что данные общие рекомендации могут быть полезными для многих предприятий и организаций, занимающимися вопросами обеспечения информационной безопасности. Они помогут не только определить величину риска и его значение на практике, но и спрогнозировать его возникновение в будущем, что позволит разработать программу действий по его минимизации.

Заключение

Мировой рынок программных технологий растет очень быстрыми темпами из года в год. Благодаря использованию сетей SDN стало удобным решение многих вопросов в различных областях и сферах жизнедеятельности человека и общества. Тем не менее вместе с развитием и техническим прогрессом увеличиваются риски и угрозы информационной безопасности, которые приводят к ряду негативных последствий. Следовательно, рассмотренные в работе методы снижения рисков помогут своевременно справиться с данной проблемой, минимизировать последствия и сохранить занимаемое положение на рынке.

ЛИТЕРАТУРА

1. Балжинням Н., Лю Ю. SDN / программно-конфигурируемые сети / сравнительные исследования сети IP // Научная дискуссия: вопросы технических наук. 2017. № 2 (42). С. 78–85.
2. Мочалова Я.В. Стратегия развития малого и среднего бизнеса в регионах РФ // Пространственное развитие территорий. Сборник научных трудов Международной научно-практической конференции. 2018. С. 393–396.
3. Макеев А.С. Основные аспекты управления рисками информационной безопасности // Молодой ученый. 2016. № 8 (112). С. 126–134.
4. Ошкина Е.В. Сетевая технология SDN (обзор, современные тенденции) // Технические науки: проблемы и перспективы. Санкт-Петербург: Свое издательство. 2017. С. 3–6.
5. Рытов М.Ю. Применение методологии STRIDE для определения угроз безопасности // Автоматизация и моделирование в проектировании и управлении. 2019. №3. С.10–18.

Журнал «Современная наука: актуальные проблемы теории и практики»