DOI 10.36622/VSTU.2023.26.1.010
УДК 004.735

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ НА БАЗЕ ТЕХНОЛОГИЙ NFV/SDN: МЕТОДИКА И АЛГОРИТМ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Н.И. Баранников, Н.Н. Мурзинов, В.Г. Юрасов, В.Ю. Остапенко

В статье рассмотрена методика повышения защищенности телекоммуникационных систем, построенных на базе технологий NFV/SDN, от атак, направленных на нарушение конфиденциальности информации. В основе методики лежит алгоритм численной оценки и регулирования рисков для каждого компонента NFV/SDN системы с учетом их специфики и возможностей злоумышленников.

Ключевые слова: NFV/SDN, риск, атака, конфиденциальность, виртуализация.

Введение

Всё больше в современные информационные технологии проникает такое понятие как виртуализация, и эта новомодная тенденция не смогла обойти стороной и телекоммуникационные системы (ТКС). Архитекторы современных ТКС уже сейчас понимают важность развития собственных решений на базе таких технологии как NFV/SND. Прямым подтверждением этому является внесение Правительством Российской Федерации в перечень наиболее приоритетных задач NFV и SDN технологии [1]. Согласно недавним исследованиям, общий объём мирового рынка NFV/SDN к 2024 году составит 88 миллиардов долларов США, что является на 42% больше аналогичного показателя для 2017 года. Также, ввиду ввода в отношении Российской Федерации большого количества санкций со стороны поставщиков телекоммуникационного оборудования, таких как Cisco и Huawei, остро встала проблема по реализации собственных решений. NFV/SDN технологии помогают решить данную проблему, так как для их реализации нет необходимости создавать сложные сетевые устройства, а необходимо разработать программно-определяемую сеть.

Однако, за быстрой популяризацией и внедрением новых современных технологий, часто следуют проблемы, связанные с информационной безопасностью [2,3]. ТКС, построенные на базе технологий NFV/SDN, не стали в этом плане исключением. Высокая востребованность современного формата сетевой структуры [4,5] влечёт за собой возникновение рисков нарушения конфиденциальности информации [6]. Сетевая инфраструктура подобного формата может включать в себя различные ресурсы, такие как IP адреса, открытые порты, VLAN виртуальных машин, сетевую топологию, что является уязвимой информацией [7]. Из всего вышеперечисленного следует вывод о серьёзности последствий нарушения конфиденциальности информации для взаимодействующих элементов NFV/SDN структуры. В связи с этим необходим программно-технический комплекс (ПТК) оценки и регулирования рисков.

В данной работе рассматриваются ТКС, построенные на базе технологий NFV/SDN, атакуемые с помощью реализации атаки проникновения в виртуальную машину. Следует отметить, что будет рассмотрена специфика взаимодействия NFV и SDN технологий, что позволит выделить исследуемую область, относящуюся к виртуальным машинам.

Актуальность работы определяется следующими факторами:

– широкая потребность государства и рынка в ТКС, построенных на базе NFV/SDN технологий, стойких к уязвимостям, связанным с использованием виртуальных машин;

©Баранников Н.И., Мурзинов Н.Н., Юрасов В.Г., Остапенко В.Ю., 2023

– необходимость разработки методического и алгоритмического обеспечения оценки и регулирования рисков нарушения конфиденциальности информации для ТКС, построенных на базе NFV/SDN технологий;

– потребность специалистов по информационной безопасности в программно-техническом комплексе для оценки и регулирования рисков нарушения конфиденциальности информации в ТКС, построенных на базе NFV/SDN технологий.

В данный момент существуют работы, посвящённые тематике безопасности в NFV/SDN. Далее перечислены темы, которые затрагиваются в аналогичных работах:

– уязвимости и возможности NFV/SDN технологий;

– уязвимости виртуализации и облачных решений на базе структуры NFV/SDN;

– модели оценки рисков нарушения безопасности в сегменте виртуализации информационной системы;

– практики по регулированию рисков, возникающих в виртуальных машинах;

– ПТК для анализа защищённости информационных систем на основе сценариев компьютерных атак.

В вышеприведённых темах широко представлены материалы по оценке рисков в системах виртуализации и регулированию рисков согласно специфики технологии NFV. Также присутствует большое количество ПТК для проверки уровня защищённости информационных систем при проведении различных атак. Однако, данные программные продукты производят анализ защищённости системы, не учитывая интеграцию между уровнями NFV модели с SDN технологией. Во время проведения сравнительного анализа моделей оценки и регулирования рисков, выявлены следующие противоречия:

– между необходимостью разработки методического и алгоритмического обеспечения для автоматизированной оценки рисков нарушения конфиденциальности информации для ТКС, использующих уязвимости NFV/SDN технологий, и отсутствием у существующих аналогов количественной оценки;

– между необходимостью создания методического и алгоритмического обеспечения риск-регулирования реализации атак проникновения в виртуальную машину, и отсутствием описания соответствующих мер для ТКС, базирующихся на NFV/SDN технологиях;

– между необходимостью повышения степени защищённости ТКС, построенных на базе NFV/SDN технологий, в условиях возникновения угроз нарушения конфиденциальности, и недостаточной эффективностью инструментария, позволяющего произвести оперативный риск-анализ объекта исследования;

Объектом исследования данной работы являются телекоммуникационные системы, построенные на базе NFV/SDN технологий, в условиях возникновения угроз нарушения конфиденциальности.

Предметом исследования является оценка и регулирование рисков успешной реализации атак, направленных на нарушение конфиденциальности компонентов ТКС, использующих технологию NFV/SDN.

Постановка задач исследования

Цель исследования данной работы заключается в повышении защищённости ТКС, построенных на базе NFV/SDN технологий, за счёт создания методического и программного обеспечения оценки и регулирования рисков реализации атак, направленных на нарушение конфиденциальности.

Для достижения поставленной цели необходимо решить следующие задачи:

1.Разработать методическое и алгоритмическое обеспечение количественной оценки рисков успешной реализации атак, направленных на нарушение конфиденциальности, для ТКС, использующих технологию NFV/SDN;

2.Создать методическое и алгоритмическое обеспечение регулирования рисков нарушения конфиденциальности информации, включая меры и средства, необходимые и достаточные для регулирования рисков в ТКС, построенных на базе технологий NFV/SDN;

3. Разработать программно-технический комплекс для автоматизированной оценки и

регулирования рисков нарушения конфиденциальности информации в ТКС, построенных на базе технологий NFV/SDN.

Анализ существующих методик оценки рисков нарушения конфиденциальности информации

Агентство Европейского союза по кибербезопасности (ENISA) в рамках проекта «Структура возникающих и будущих рисков» описало ключевые риски безопасности структур облачных вычислений. В 24 подпункте 1 пункта рассмотрены риски, возникающие в облаках, в том числе и нарушения конфиденциальности информации. Среди описанных рисков выделялись:

– потеря доверия к облачным провайдерам;

– нарушение изоляции в виртуализированной инфраструктуре;

– потеря конфиденциальной информации при переносе инфраструктуры между облачными провайдерами;

– небезопасное и неполное удаление данных в облачной инфраструктуре.

Во 2 пункте данного документа содержится аппарат оценки рисков. Оценка происходит с использованием следующей информации:

– возможность проведения атаки на данную информационную систему;

– способ виртуализации, с помощью которого реализована атакуемая информационная система;

– возможный ущерб от атаки.

Однако, отсутствует методика по регулированию рисков для технологий NFV/SDN, с помощью которых построен наш объект исследования.

Устоявшимся способом регулирования рисков можно считать метод CRAMM. Оценка происходит как с использованием количественных, так и качественных характеристик и осуществляется присваиванием оценки по десятибалльной шкале. Анализ выполняется с использованием нескольких параметров, в которых учитываются оценки, присвоенные информационным ресурсам. В рамках метода CRAMM можно выделить несколько видов ущерба, которые относятся к NFV/SDN сетям:

– ущерб, связанный с разглашением персональных данных отдельных лиц;

– потери, связанные с восстановлением ресурсов;

– потери, связанные с невозможностью выполнения обязательств, которые определяли облачные провайдеры.

Оценка происходит как с использованием количественных, так и качественных характеристик и осуществляется присваиванием оценки по десятибалльной шкале. Весь процесс оценки рисков с использованием метода CRAMM делится на несколько пунктов:

– определение уровня критичности;

– проведение анализа безопасности ИС, который формируется посредством сбора статистики у лиц, имеющих доступ к информации по атакам;

–анализ рисков и выявление контрмер по их противодействию.

Вышеописанный подход требует доработок ввиду того, что параметры ущерба не полностью описаны для NFV/SDN ТКС, в частности не приведён алгоритм по определению критичности компонентов системы.

Описание методики численной оценки рисков нарушения конфиденциальности информации

В данном пункте будем использовать ранее описанную методику от ENISA для оценки рисков в облачных структурах. Однако, если попробовать её применять к схеме взаимодействия компонентов системы, то можем столкнуться с проблемой невозможности проведения полной количественной оценки рисков, так как сама методика ориентирована на качественные методы.

Для проведения количественной оценки рисков необходимо идентифицировать следующие системные параметры на основе рассмотренных особенностей NFV/SDN технологий:

– идентификация активов на стыке NFV/SDN технологий. Выделение их в компоненты;

– выявление уязвимостей у компонентов NFV/SDN ТКС;

– вероятность возникновения угроз нарушения конфиденциальности информации;

– оценка риска нарушения конфиденциальности информации для каждого информационного актива с учётом успешной реализации атаки;

Подробно рассмотрим категории данных, которые циркулируют в данной ТКС:

– сетевые параметры взаимодействующих устройств;

– конфигурационные параметры сети;

– статистика маршрутизируемого трафика до конечной точки;

– информация о местонахождении конечного пользователя;

– параметры виртуальных сетевых функций;

– данные для корректной работы виртуальных сетевых функций.

Согласно исследованиям в области риск-анализа [8], оценить риск нарушения конфиденциальности информации можно, рассчитав произведение численной оценки вероятности успешной реализации атаки и ущерба, который возникает при воздействии этой атаки на систему по формуле (1):

$$risk = r \times s, \tag{1}$$

где s – ущерб, возникающий при успешной реализации атаки;

r – вероятность возникновения ущерба.

Вероятность возникновения ущерба для телекоммуникационных систем, построенных на базе технологий NFV/SDN должно представлять нормальное распределение для каждой из атак, которая направлена на нарушение конфиденциальности информации [9]. Для атак, которые выполняются больше 100 раз на протяжении времени t, такие как внедрение инъекций средствами Nmap, r описывается по формуле (2):

$$r = \frac{e^{\frac{-(k-m*s*t)^2}{2m}}}{\sqrt{2\pi s(s_{max}-s)}}, \tag{2}$$

где m – общее число реализуемых атак;

k – число успешно реализуемых атак;

s – ущерб от атаки;

s_{max} – максимальное значение ущерба, имеет значение 1;

t – параметр времени.

Для атак, которые реализуются с постоянной интенсивностью на NFV/SDN компонент, такие как ip spoofing, представляется возможным использовать формулу Пуассона (3):

$$r = \frac{s * (\lambda_0 * t)^m}{m!} e^{-\lambda_0 * t} \tag{3}$$

где$\lambda_0 = \frac{t}{t_0}$ – приведённая интенсивность, среднее число атак за исследуемый интервал времени;

t_0 – среднее значение временного интервала между атаками;

t – исследуемый промежуток времени;

m – общее число реализуемых атак;

s – ущерб от атаки.

Последним нерассмотренным компонентом в данной формуле остался ущерб s, который считается по формуле (4) [10]:

$$s = f_{norm}(v \times l), \tag{4}$$

где v – количественный уровень ущерба от атаки;

l – коэффициент поправки для NFV/SDN компонента;

f_{norm} – функция нормирования по максимальным значениям произведения v_{max} l_{max} для получения безразмерной оси ущерба;

s – ущерб от реализации атаки.

Ущерб от реализации атак вычисляется с помощью произведения: количественный уровень ущерба от атаки v на коэффициент поправки для NFV/SDN компонента l.

Уровень ущерба v от реализации угроз нарушения конфиденциальности информации оценивается следующим образом:

– минимальный ущерб (М) – данный ущерб не приводит к материальным или репутационным потерям телекоммуникационной компании. Значение 1;

– умеренный ущерб (У) – потеря подобного рода информации ведёт к умеренной потере репутационных и материальных ресурсов. Значение 3;

– средний ущерб (С) –данный ущерб ведёт к потере существенной информации и несёт материальные и репутационные убытки. Значение 5;

– большой ущерб (Б) – потеря подобного рода информации ведёт к большим материальным потерям со стороны телекоммуникационных провайдеров и ведёт к большому репутационному ущербу. Возможен уход клиентов. Значение 7;

– критический ущерб (К) – максимальный уровень ущерба который ведёт к отказу клиентов от услуг провайдера для данной виртуализированной функции. Значение 10.

Параметр l определяется следующим образом:

– для уровня приложения – 0.02 (М), 0.04 (У), 0.06 (С), 0.08 (Б), 0.1(К);

– для уровня управления – 0.01(М), 0.03 (У), 0.05 (С), 0.07 (Б), 0.9 (К);

– для уровня инфрастуктуры – 0.01 (М), 0.03 (У), 0.05 (С), 0.06 (Б), 0.8 (К); Результаты оценки риска представлены в табл. 1.

Таблица 1

Данные для расчета показателя риска нарушения конфиденциальности информации NFV/SDN компонентов

NFV/SDN компонент	Тип информации	Реализуемая атака	$risk$	s
Микросервис аналитики(приложение)	Повышение привилегий при помощи ПТК Angler	Обработанные и классифицированные на уровне мониторинга данные	0,56	0,81
Объект Мониторинга (приложение)	Применение программы типа Cain&Abel	Сетевые метрики Данные о местонахождении пользователя	0,52	0,79
Объект конфигурации (приложение)	Внедрение инъекций средствами Nmap	Топология SDN сети	0,76	0,8
Связь с уровнем инфраструктуры (управление)	Атаки DRAMA	Параметры взаимодействия компонентов	0,41	0,76
	Атаки типа DHCP Starvaton	Таблицы коммутации, хранящие MAC адреса	0,45	0.53
Маршрутизатор (инфрастуктура)	Атаки типа IP spoofing	Таблицы маршрутизации, хранящие IP адреса	0,49	0.53

В рассмотренной модели представлена обобщённая схема взаимодействия компонентов. Алгоритм для проведения оценки риска нарушения конфиденциальности информации NFV/SDN представлен на рис. 1.

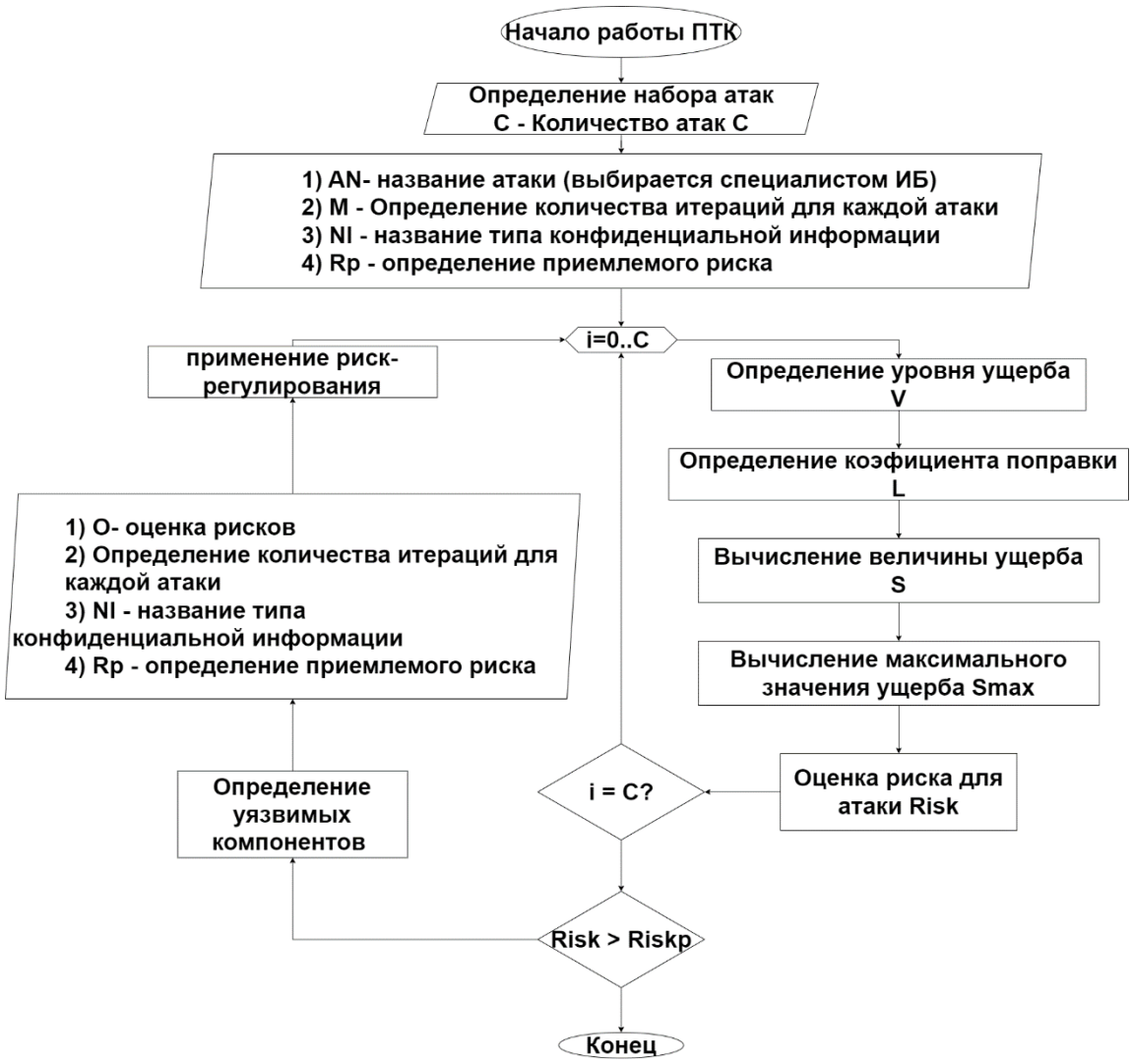

Рис. 1. Алгоритм оценки риска нарушения конфиденциальности информации

Описание методики численной оценки рисков нарушения конфиденциальности информации

Риск- регулирование будет представлять процесс снижения текущей оценки за счёт применения соответствующих мер. Данная работа представляет методику, которая содержит в себе существующие практики, адаптированные под ТКС, построенные на базе NFV/SDN ТКС.

Существующие практики по регулированию рисков, такие как методика от ФСТЭК России MITRE ATT&CK, могут быть применены в телекоммуникационных сетях, использующих NFV/SDN технологии. За основу возьмём методику, которую представила организация Cloud Security Alliance в 2015 году для регулирований рисков в системах, которые базируются на виртуальном окружении [11].

Для каждого из уровней SDN системы определим набор мер и обозначим их в соответствии с компонентами, где:

П – меры по регулированию рисков на уровне приложения;

У – меры по регулированию рисков на уровне управления;

И – меры по регулированию рисков на уровне инфраструктуры;

Для полученных компонентов из методики оценки рисков опишем меры по регулированию.

Для компонента аналитики данных применимы следующие меры:

– шифрование данных, которые используются в аналитике и хранятся на виртуальных и облачных серверах. (П1);

– применение политик для ограничения хранения образов виртуальных машин и моментальных снимков компонента аналитики (П2);

– подключение системы регистрации действий с целью обзора или аудита действий в системе (П3);

– использование проверенных библиотек и использование актуальных, поддерживаемых версий фреймворков (П4);

Для компонента мониторинга данных применимы следующие меры:

– шифрование данных, которое будет основываться на политиках доступа в систему (П5);

– использование предусмотренных для потоковой передачи данных хранилищ, таких как системы управления базами данных. (П6);

– минимальное журнализирование конфиденциальной информации внутри логики компоненты мониторинга (П7);

– в случае использования систем контейнеризации, создание реестра наиболее стабильных, проверенных образов компоненты системы, с минимально допустимыми уязвимостями (П8).

Для объекта настройки и хранения конфигурации применимы следующие меры:

– оптимизировать количество используемых сущностей базы данных на окружении с целью минимизации дублирования конфиденциальной информации о состоянии топологии сети (П9);

– разнесение виртуальной сетевой логики согласно микросервисной структуры (П10);

– шифрование хранимой конфигурации на основе политик доступа в систему (П11);

– использование проверенных библиотек и использование актуальных, поддерживаемых версий фреймворков при написании программной логики (П12);

– использование многофакторной и/или раздельной проверки подлинности (П13).

Меры по регулированию рисков в центральном контроллере связи с уровнем инфраструктуры:

– контроль виртуальной сети и трафика данных аналогично физическим сетям (У1);

– внедрение технологий безопасности, охватывающих физические и виртуальные среды, которые согласованны с системой управления политиками, и обеспечения их соблюдения (У2);

– производство взаимодействий с каждым из компонентов нижележащего уровня по частному API (У3).

Меры по регулированию рисков для объекта, выполняющего функции коммутации:

– разработка более строгих правил конфигурирования гипервизора, чтобы уменьшить области уязвимости (И1);

– отключение неиспользуемых физических аппаратных устройств и оптимизация буфера обмена со службами общего доступа к файлам (И2);

– при загрузке гипервизора проводить проверку целостности (И3);

– использовать упреждающий мониторинг для обнаружения несанкционированных действий и нарушений конфиденциальности информации (И4).

Для объектов, выполняющих функции маршрутизации, применимы следующие меры по регулированию рисков:

– применение и обновление практик поставщиков гипервизора по защите конфиденциальной информации (И5);

– использование административных средств управления, исходя из ролей и потребностей пользователей (И6);

– разделение виртуальных машин путем создания зон безопасности, стадии производства и чувствительности данных на отдельных физических кластерах аппаратных компонентов (И7).

После переоценки рисков нарушения конфиденциальности информации имеем результаты, показанные на рисунке 2.

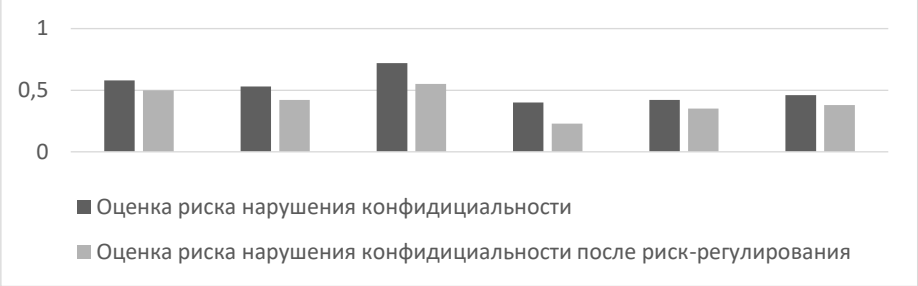

Рис. 2. Показатели оценки рисков нарушения конфиденциальности информации в ТКС, базирующихся на технологиях NFV/SDN

Способ реализации программно-технического комплекса оценки и регулирования рисков

– клиентская часть – компонент, который взаимодействует с пользователем. Чаще всего реализуются с помощью таких фреймворков как React, AngularJS, Vue;

– серверная часть ответственна за внутреннюю логику приложения и используется для базирования на различных web фреймворках в зависимости от используемого языка программирования. Будет использоваться для реализации логики оценки рисков;

– база данных – постоянное хранилище, к которому обращается серверная часть для получения данных, необходимых в логике приложения;

Данный способ построения программного обеспечения подходит для реализации поставленных задач. В дополнение ко всему вышеописанному, можно отметить, что для ПТК оценки и регулирования рисков нужно использовать дополнительные утилиты, необходимые для риск-анализа и риск регулирования.

Для построения ПТК возможно воспользоваться описанием 8 модулей, представленных в табл. 2

Таблица 2

Модули ПТК оценки и регулирования рисков

Модули	Функции модулей
Модуль формирования запросов оценки рисков (Визуальный интерфейс)	Сбор информации с визуальных компонентов системы и данных
Модуль отображения оценки рисков (Визуальный интерфейс)	Отображение результатов в пользовательском интерфейсе
Модуль авторизации и аутентификации (Серверная сторона)	Реализация авторизированного взаимодействия между клиентом и сервером
Модуль формирования атак (Серверная сторона)	Подготовка начальных данных, необходимых для оценки рисков
Модуль оценки рисков (Серверная сторона)	Реализация методики по оценке рисков и соответствующего алгоритма
Модуль регулирования рисков (Серверная сторона)	Проведение риск-регулирования согласно описанной методики
Модуль формирования и предоставления отчёта (Серверная сторона)	Формирование результатов после проведения процесса риск-анализа, риск-регулирования
Модуль предоставления информации (Система управления базами данных)	Предоставляет информацию для процесса оценки и регулирования рисков.

Заключение

Предложенная в статье методика повышения защищенности телекоммуникационных систем, построенных на базе технологий NFV/SDN, от атак, направленных на нарушение конфиденциальности информации, разработана на основе алгоритма оценки рисков для каждого компонента NFV/SDN системы. В работе представлена логическая модель, учитывающая особенность архитектуры построения телекоммуникационных систем, базирующихся на технологиях NFV/SDN, модель угроз, включающая описание возможностей злоумышленников и атак для каждого компонента телекоммуникационной системы, предложен инструментарий численной оценки и регулирования рисков с примером автоматизации. Полученные результаты в виде численной оценки рисков нарушения конфиденциальности информации позволяют выполнять анализ для каждого компонента системы, и на этой основе проектировать программно-технические комплексы, сигнализирующие об уязвимых участках NFV/SDN телекоммуникационных систем и соответствующих угрозах нарушения конфиденциальности информации.

Предложенные алгоритмы оценки и регулирования рисков нарушения конфиденциальности информации в телекоммуникационных системах, построенных на базе NFV/SDN, могут быть использованы для проверки уровня защищённости.

Список литературы

1. О приоритетных научных задачах, для решения которых требуется задействовать возможности федеральных центров коллективного пользования (ФЦКП) научным оборудованием // 26.02.2014. URL: https://fea.ru/news/5787 (дата обращения 15.02.23).

2. Ермаков С.А. Комплексный анализ систем интернета вещей для выявления уязвимостей в контексте обеспечения информационной безопасности / С.А. Ермаков, А.А. Болгов // Информация и безопасность. 2022. Т. 25. Вып. 2. С. 219-225.

3. Ермаков С.А. Обзор существующих процедур контроля доступа в контексте обеспечения безопасности систем интернета вещей / С.А. Ермаков, А.А. Болгов // Информация и безопасность. 2022. Т. 25. Вып. 2. С. 231-239.

4. Остапенко А.Г. К вопросу о трендах и инструментарии социо-информационного глобального противоборства [Текст] / А.Г. Остапенко, А.А. Остапенко, Н.М. Лантюхов, С.Д. Трубицын, И.А. Боков // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 519-524.

5. Остапенко А.Г. «Инфодемия» и социальные сети: актуальные объекты и задачи исследования / А.Г. Остапенко, Р.В. Сорокин, С.В. Лихобабин, А.О. Ткаченко, А.Н. Бартенев, Ю.Г. Пастернак // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 535-544.

6. Остапенко А.Г. Краткие научно-методические рекомендации по формированию и выполнению технических заданий в области обеспечения информационной безопасности / А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.А. Остапенко, А.В. Заряев, Т.Ю. Мирошниченко, П.Д. Федоров // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 551-560.

7. Остапенко А.Г. «Инфодемия» и социальные сети: модели эпидемического процесса / А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, Д.А. Нархов, П.Д. Федоров, Р.В. Сорокин // Информация и безопасность. 2020. Т. 23. Вып. 2. С. 285-290.

8. Сердечный А.Л. Риск-анализ и прогнозирование частоты и ущербности компьютерных атак. / А.Л. Сердечный, А.С. Маликова, А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.Н. Бартенев. // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 159-178.

9. Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Проникновения в операционную среду компьютера: модели злоумышленного непосредственного доступа. 2013. С. 119-120.

10. ENISA. Методический материал Оценка рисков в облачных вычислениях. 2019. С. 5-11.

11. Cloud Security Organization. Практики по регулированию рисков, возникающих в виртуализированной среде. 2013. С. 8-15.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 26.02.2023

Информация об авторах

Баранников Николай Ильич – д-р. техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Мурзинов Николай Николаевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Юрасов Владислав Георгиевич – д-р. техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Остапенко Владимир Юрьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

IMPROVING THE SECURITY OF TELECOMMUNICATION SYSTEMS BASED ON NFV/SDN TECHNOLOGIES: METHODOLOGY AND ALGORITHM FOR ASSESSING THE RISKS OF INFORMATION PRIVACY VIOLATIONS

N.I. Barannikov, N. N. Murzinov, V.G. Yurasov, V.Yu. Ostapenko

The article discusses a technique for improving the security of telecommunication systems built on the basis of NFV/SDN technologies from attacks aimed at violating the confidentiality of information. The methodology is based on an algorithm for numerical assessment and risk management for each component of the NFV/SDN system, taking into account their specifics and the capabilities of intruders.

Key words: NFV/SDN, risk, attack, privacy, virtualization.

Submitted 26.02.2023

Information about the authors

Nikolay I. Barannikov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Nikolay N. Murzinov – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Vladislav G. Yurasov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Vladimir Yu. Ostapenko – student, Voronezh State Technical University, e-mail: mnac@comch.ru