Моделирование и анализ информационных систем. Т. 26, №1 (2019), с. 134–145
Modeling and Analysis of Information Systems. Vol. 26, No 1 (2019), pp. 134–145

DOI: 10.18255/1818-1015-2019-1-134-145

УДК 004.056.5(076)

«Общие критерии» и безопасность программно-конфигурируемых сетей

Петухов А. Н., Пилюгин П. Л.

Поступила в редакцию 10 января 2019
После доработки 17 февраля 2019
Принята к публикации 18 февраля 2019

Аннотация. «Общие критерии» (ISO 15408) – общепризнанный и широко применимый подход к управлению и оценке решений в области информационной безопасности. «Общие критерии» опираются на разработку общей концептуальной основы для ключевых решений безопасности, включая профили защиты и целевые объекты безопасности. Концептуальная основа разработки подразумевает определение следующих элементов: цели и предположения безопасности (для среды и объекта), угрозы и политики безопасности, а также функциональные требования и требования к обеспечению безопасности. Специфика решений по обеспечению безопасности SDN во многом обусловлена фундаментальными архитектурными принципами самой технологии SDN – в первую очередь разделением потоков управления и данных, а также условиями применения протокола OpenFlow. Тем не менее, проактивные (угрозы и политики), пассивные (цели и предположения) и реактивные (требования) аспекты управления безопасностью остаются весьма актуальными для такого типа решений безопасности. В статье рассматриваются особенности применения единых критериев оценки безопасности SDN и практического опыта Московского технического университета связи и информатики при разработке профиля защиты. Новый класс сетевых атак на коммутаторы и контроллеры SDN может использовать как данные, так и компоненты управления. В дополнение к традиционным уязвимостям централизация функций управления открывает путь для новых угроз безопасности путем изоляции деятельности контроллера и обмена управляющими сообщениями. Поэтому выявление и анализ угроз, политик и требований, специфичных для безопасности модуля управления SDN, становится новым приоритетом.

Ключевые слова: безопасность программно-конфигурируемых сетей, общие критерии, профиль защиты

Для цитирования: Петухов А. Н., Пилюгин П. Л., "«Общие критерии» и безопасность программно-конфигурируемых сетей", *Моделирование и анализ информационных систем*, **26**:1 (2019), 134–145.

Об авторах:
Петухов Андрей Николаевич, канд. техн. наук, orcid.org/0000-0002-1427-2440
Национальный исследовательский университет «МИЭТ»
пл. Шокина, 1, г. Зеленоград, г. Москва, 124498 Россия, e-mail: anpetukhov@yandex.ru

Пилюгин Павел Львович, канд.техн. наук, orcid.org/0000-0003-0011-7180
Московский государственный университет имени М.В. Ломоносова,
Ленинские горы, 1, г. Москва, 119991 Россия, e-mail: ppl@mail.ru

Благодарности:
Работа выполнена при поддержке ректората Московского технического университета связи и информатики (МТУСИ): С. Д. Ерохина, Ю. Л. Леохина и А. Ю. Муханова — и при финансировании МТУСИ по направлению «Безопасность критических информационных инфраструктур».

Введение

В статье рассматриваются результаты анализа факторов нарушения информационной безопасности программно-конфигурируемых сетей (ПКС), целей, задач и требований безопасности для среды и условий функционирования ПКС как объекта оценки в рамках концепции «Общих критериев» [1].

1. Профиль защиты

Осмысленное обеспечение любой безопасности предполагает наличие адекватного представления об опасности. В каждом конкретном случае есть специфика структуры и формы такого представления, но общими элементами всегда являются:

– типология проявления опасности, номенклатура идентифицированных и квалифицированных видов такого проявления, внешних (агрессивность среды) и внутренних (несовершенство объекта) событий и ситуаций, являющихся причиной возникновения ущерба (проактивный аспект);

– совокупность и структура активов (объектов и процессов), подвергающихся опасности, речь идет о пространстве информационных ресурсов, их состояний и взаимодействий, а также о характере их подверженности опасности (пассивный аспект);

– элементы и свойства объекта (средства защиты, особенности архитектуры, ограничивающие решения и т.п.), препятствующие реализации опасности (реактивный аспект).

На базе таких сведений строится модель угроз, проводится анализ и управление рисками, исследуются уязвимости, учитываются инциденты, эти данные используются при формировании политик безопасности.

Одним из эффективных форматов использования этих сведений для решения проблем безопасности является профиль защиты. Понятие профиля защиты восходит к концепции управления информационной безопасностью с привлечением моделирования требований и условий (не только для объекта управления, но и для среды его функционирования), а также оценки доверия к средствам реализации этих условий и способам выполнения этих требований («исчисление доверия»). Базовым изложением этой концепции является международный стандарт ISO/IEC 15408-1:2005. (т.н. «Общие критерии») [1].

В профиле защиты стандартом предусмотрено несколько категорий, которые в совокупности исчерпывающе отображают все три аспекта представления об опасности и дают возможность обоснованно выстроить систему защитных мер. В качестве средства отображения проактивного аспекта профилем защиты используется категория *«угрозы»*, которая в стандарте полагается высокоуровневой (т.е. первичной) сущностью, гармонизированной (т.е. взаимодействующей, согласованной, обусловливающей и обусловливаемой) с такими высокоуровневыми сущностями, как «активы», «злоумышленники», «уязвимости» и «риски». Для выражения пассивного

аспекта привлекается производная категория *«предположения»*, с помощью которой ограничивается пространство информационных активов и специфицируется интерфейс с окружающей средой. Кроме того, *«предположения»*, отнесенные к внутренним свойствам и характеристикам, отчасти поддерживают реактивный аспект. Основным же инструментом для представления реактивного аспекта в профиле защиты является категория *«политики»*, которая соответствует возможностям (реализованным и гипотетическим) противодействовать вредоносным факторам агрессивной среды. Для обеспечения взаимной корректности *«угроз», «предположений» и «политик»* в профиле защиты предусматривается специальный механизм, выраженный в виде *«целей безопасности»* для среды и самого объекта.

2. Локализация сервисов безопасности

В сетях традиционной архитектуры основным (но не единственным) применяемым подходом к обеспечению безопасности является вынесение функций безопасности в отдельный компонент-посредник, осуществляющий инспекцию и модификацию трафика, принятие решений, аудит и т.п. (межсетевой экран, IDS/IPS, VPN, VLAN и др.), и вынесенный физически или концептуально в отдельный элемент сети. ПКС не исключает такого подхода, например, в [2] предлагается использовать контроллер для управления вынесенными сервисами безопасности. В этом случае приложения указывают контроллеру, какие функции безопасности должны быть активизированы на том или ином узле-посреднике, расположенном между контроллером и сетью. Таким образом, эти приложения расширяют возможности контроллера путем вынесения функций безопасности за его пределы.

Другой подход [3] к использованию локализованных сервисов безопасности ПКС предполагает взаимодействие устройства-посредника с контроллером посредством специального программного интерфейса. В заголовки пакетов внедряются специальные теги, содержащие информацию о потоке, что позволяет обеспечить контролируемую маршрутизацию этого потока на устройство-посредник и его дальнейшую обработку на нем. Процедура работает на базе предварительно программируемых политик, что делает невозможным динамическую модификацию функций безопасности. Развитием такой схемы [4] является построение механизма трансляции высокоуровневых политик безопасности в правила конфигурирования конечных коммутаторов на узлах-посредниках.

Функции безопасности, реализуемые на узлах-посредниках, предназначены для противодействия угрозам, направленным на линии связи, коммуникационное оборудование и узлы сети:

– Межсетевые экраны для защиты периметра и контроля внутреннего домена.

– Системы обнаружения и предотвращения вторжений, которые контролируют сетевые активности для обнаружения вредоносных действий или нарушений политики безопасности и пытаются предотвратить атаки.

– Виртуальные частные сети (SSL VPN), которые обеспечивают безопасное разделение клиентов и доменов.

– Решения для управления сетью, которые позволяют централизованно управлять многими из функций безопасности через консоль администратора.

– IEEE 802.1X – проверка подлинности и контроль доступа к сети на основе портов (VLAN).

– IPsec для сквозной проверки подлинности и шифрования IP-пакетов в сеансе связи.

– Безопасность транспортного уровня (TLS) для шифрования коммуникаций уровня приложения.

– Безопасность транспортного уровня (TLS) для криптографической защиты коммуникаций между приложениями на транспортном уровне.

– Сервис удаленного доступа пользователя (RADIUS) – сетевой протокол, который обеспечивает централизованное управление аутентификацией, авторизацией и учетом (AAA) для конечных устройств, использующих сетевые услуги.

Неизбежной платой за локализацию функций безопасности, заимствованную у традиционных сетей, и вынесение механизмов реализации этих функций за периметр контроллера являются определенные потери производительности при перенаправлении трафика на дополнительные устройства, что затрудняет применение этого подхода в сетях, чувствительных к задержке.

Для описания безопасности сетевой инфраструктуры и управления сетевыми сущностями на уровне узлов-посредников созданы профили защиты для различных типов межсетевых экранов и систем обнаружения вторжений. Например, в отношении ПКС для контроля потоков плоскости данных практически без доработки могут применяться профили защиты межсетевых экранов уровня логических границ (VLAN) или хостов внутри сети, а также профили защиты систем обнаружения вторжений уровня узла. Эти решения снабжены гармонизированными *«целями безопасности»* для среды и объекта в условиях актуальных *«угроз»* безопасности, для них сформулированы наборы *«предположений»*, позволяющие интегрировать их в состав сетей с различными уровнями и границами доверия. Опытом применения этих профилей защиты практически решены проблемы трансляции *«политик»* безопасности в нотации конфигурационных файлов и других инструментов настройки. Дополнительно отметим, что даже при централизованной инкапсуляции функций безопасности более точно назначению и роли контролера ПКС соответствуют именно системы обнаружения вторжений, которые централизованно собирают и анализируют информацию о состоянии узлов сети (это соответствует системам обнаружения вторжений уровня сети).

Особенности OpenFlow ограничивают возможности применения предопределенных (типовых) профилей защиты для контроля сетевых транзакций плоскости управления. Однако доработка профилей защиты, которая необходима для такого применения, может оказаться незначительной и коснуться лишь той части *«функциональных требований»*, которые непосредственно включают указания на *«атрибуты безопасности»*, т.е. используются для настройки сервисов безопасности на базе узлов-посредников. Это обстоятельство возможно в редком случае совпадения

«угроз», *«целей безопасности среды»* и *«предположений»* для потоков плоскости управления и плоскости данных.

3. Централизованная инкапсуляция сервисов безопасности

Одно из принципиальных архитектурных решений ПКС – это разделение сетевых сервисов для функций управления и функций пересылки пакетов. Согласно концепции ПКС, вся функциональность управления выносится в контроллеры, которые способны отслеживать работу всей сети и управлять сетевыми коммутаторами, выполняя планирование и управление трафиком с использованием программных приложений (что и определило название технологии). Этим обстоятельством можно воспользоваться для организации сервисов безопасности. Однако централизация управления в свою очередь способствует возникновению проблем безопасности, так как, в дополнение к традиционным атакам, обособленность функционирования контроллера и циркуляции сообщений в плоскости управления приводят к возникновению новых угроз безопасности [5], причем новый класс сетевых атак на коммутаторы и контроллеры ПКС возможен как из плоскости данных, так и в плоскости управления.

Рассмотрение безопасности протоколов (включая формирование угроз, политик и требований) целесообразно осуществлять раздельно по направлениям безопасности протокола контроллер – коммутатор (в том числе для аспектов, выходящих за пределы базового уровня, обеспечиваемого локализованными сервисами), безопасности протоколов управляющих приложений и безопасности протоколов контроллер – контроллер.

Анализ структуры устройств и использование модели STRIDE для идентификации угроз позволили сформулировать следующее общее описание угроз для ПКС [6, 7]:

– *Фальсифицированные потоки трафика*: потоки, созданные неисправными или дублирующими устройствами в сети, которые могут использоваться для отказа в ресурсах другим устройствам, либо в плоскости управления, либо в плоскости данных.

– *Эксплуатация уязвимостей коммутаторов*: попытки использования уязвимостей в коммутаторах, чтобы скомпрометировать эти устройства; такие атаки могут привести к другим уязвимостям в сети.

– *Атаки на управляющий канал связи*: любая атака, которая может поставить под угрозу безопасность канала связи между плоскостью данных и плоскостью управления, может нарушить или даже остановить сетевые операции; другие атаки могут просто попытаться перегрузить канал связи, чтобы предотвратить функционирование сети.

– *Использование уязвимостей контроллера*: аналогичны атакам на уязвимости коммутаторов, но гораздо более серьезны; после того как контроллер скомпрометирован, злоумышленник потенциально имеет полный контроль над сетью.

– *Нарушение доверия между контроллерами и приложениями*: большинство контроллеров не устанавливают правила доверия для приложений и не поддерживают механизмы для установления доверия; приложения, запущенные на контроллерах, должны быть доверенными, так как приложение контроллера имеет такое же представление о сети, как и контроллер.

– *Утрата надежности на станциях администрирования*: контроллер должен быть защищен от атак в сети, так же как и средства управления контроллером; если эта система скомпрометирована, злоумышленник может перепрограммировать контроллер, а не пытаться скомпрометировать его.

Эти направления являются основой для формирования проактивного аспекта в профиле защиты для централизованно инкапсулированных сервисов безопасности. Угрозы контроллеру рассматриваются по всем возможным интерфейсам: со стороны приложений, систем управления и устройств сети. Угрозам подвергаются критические информационные ресурсы контроллера, нарушается его работоспособность, на нем осуществляется захват управления. Важно отметить, что другие сетевые устройства и каналы связи в таком профиле защиты не рассматриваются в соответствии с выбранной архитектурой сервисов безопасности. Для них сформулированы соответствующие *«предположения»* защиты, которые ограничивают информационные ресурсы, безопасность которых является прерогативой разрабатываемого профиля защиты (пассивный аспект). Этими *«предположениями»* фактически определяется и поддерживается состав критически важных активов контроллеров ПКС, подлежащих защите [7]:

– Данные учетной записи пользователя и другие учетные данные (например, пароли, сертификаты и т.д.).

– Данные конфигурации и управления (например, ресурсы и политики администрирования; IP-адрес контроллера, порты, версия протокола и т.д.).

– Данные журналов регистрации.

– Операционная система (хостовая ОС).

– Программное обеспечение, включая программное обеспечение контроллера и прикладное программное обеспечение.

– Аппаратное обеспечение (например, плата, блок питания и т.д.), используемое для запуска программного обеспечения контроллера или приложений.

– Ресурсы (например, емкость процессора, возможность обработки памяти и т.д.)

– Интерфейсы контроллеров, включая интерфейс удаленного доступа между контроллером и системой администрирования.

Эти данные являются основой для формирования пассивного аспекта профиля защиты.

Примерами *«целей безопасности»* для профиля защиты ПКС в условиях централизованной инкапсуляции сервисов могут быть поддержание изоляции данных, предотвращение эксплуатации уязвимостей, предупреждение исчерпания ресурсов и др. (перечень не претендует на полноту).

Любая технология коллективного использования системных ресурсов требует изоляции пользовательских данных друг от друга. *«Цель безопасности»* должна учитывать, на каких уровнях модели обработки данных имеет место одновременное участие нескольких пользователей в вычислительном процессе – на уровне инфраструктуры (каналы, коммутаторы), на уровне платформы (контроллеры) или на уровне приложения. Механизмы достижения такой цели – *«политики»* и *«функциональные требования»*, должны выявлять и компенсировать фрагменты технологии, не поддерживающие разделение мандатов и (или) партиционирование, в которых один аппаратный модуль (например, процессор контроллера), фрагмент кода базового программного обеспечения (например, программ формирования таблиц потоков) или экземпляр прикладного приложения (процесс) используется несколькими различными пользователями параллельно.

Передаваемые и хранимые ПКС данные могут быть скомпрометированы или фальсифицированы в обход правил и процессов обеспечения безопасности в результате эксплуатации возможных уязвимостей на различных уровнях. Информация о таких уязвимостях может оказаться общедоступной до того, как проблема будет решена. *«Цель безопасности»*, устраняющая этот риск, может достигаться путем шифрования передаваемых и хранимых данных. Разумеется, соответствующими *«политиками»* и *«функциональными требованиями»* должно быть обеспечено управление ключами и сертификатами, используемыми для шифрования данных.

Поскольку превышение интенсивности запросов к службам над максимально допустимой нагрузкой может привести к недоступности сети для пользователей, соответствующая *«цель безопасности»* может быть выражена в виде гарантий для параметров доступности сети и/или восстановления ее в случае нарушения этих гарантий.

Сложился общий набор принципов, которым должны удовлетворят средства обеспечения безопасности контроллера [7]:

– *Ограниченная доступность контроллера.* Контроллер ПКС – это централизованное решение, атаки на контроллер и приложения очень опасны, поэтому доступ к контроллеру и его приложениям должен строго контролироваться.

– *Создание доверия.* Очень важны защита целостности топологий ПКС, а это означает, что контроллер, приложения и устройства, которыми он управляет, – все должны быть доверенными.

– *Надежная структура управления.* Структура управления должна обеспечивать развертывание ПКС в соответствии с требованиями проекта. Для обеспечения доступности и безопасности необходимо урегулировать возможные конфликты нескольких сетей ПКС под одним и тем же контроллером.

– *Безопасность базовой инфраструктуры.* Программируемые сети могут использовать виртуализации сетевой инфраструктуры для подключения сервиса

на основе использования физических и виртуальных ресурсов. Инфраструктуры ПКС должны быть устойчивыми к DOS-атакам на системы управления, потоки данных пользователей и управления, на приложения.

– *Мониторинг безопасности.* ПКС представляют собой объект, который сложно контролировать. В контексте этой динамически меняющейся сетевой топологии необходимо анализировать информацию счетчиков трафика, статистику в коммутаторах, журналы контроллеров и, возможно, даже трафика в плоскости данных. Также должно контролироваться использование ПКС-API (через ведение журнала обращения приложений). Большой объем данных из различных источников, и динамический характер сети могут потребовать разработки новых методов мониторинга и анализа (например, аналитики больших данных).

– *Защита интерфейса ПКС - API.* Необходимо обеспечить безопасность интерфейса с приложениями, включая проверку подлинности и авторизацию приложений, использующих его, а также предотвращение конфликтов между приложениями. API – это направление атак, которое может позволить приложениям поражать контроллер сети или другие приложения.

Перечисленные направления являются основой для создания *«политик»* (реактивного аспекта) в профиле защиты. Эти *«политики»* в профиле защиты должны гарантировать проектирование безопасности таким образом, чтобы контроллеры ПКС не являлись слабым звеном сети и не допускали возможность компрометации. *«Политики»* включают использование защищенных протоколов, шифрование трафика коммуникаций, реализацию взаимной аутентификации, управление доступом к сервису и др.

4. Функциональные требования безопасности

Различные конфигурации границ и уровней доверия предусматривают рассмотрение сети в разных вариантах [5]:

– в рамках одного пространства доверия – все компоненты принадлежат и управляются одним и тем же субъектом; граница доверия специфицирована и совпадает с периметром сети (режим «А»);

– сеть (возможно распределенная) принадлежит одному субъекту, а приложения ПКС могут принадлежать тому же субъекту, но разрабатываться и публиковаться могут другими субъектами или целой иерархией субъектов-разработчиков приложений; граница доверия специфицирована, но не совпадает с периметром сети, а проходит внутри него (режим «Б»);

– ПКС образует облачную структуру, т. е. допускается, кроме сторонних разработчиков приложений контроллера данной сети, использовать в качестве приложений другие виртуальные ПКС со своими контроллерами, приложениями и системой администрирования, граница доверия не специфицирована (режим «В»).

В настоящей статье в качестве базового рассматривается режим «А» использования сети (один провайдер), когда вся сетевая инфраструктура, средства вычислительной техники, коммуникационное оборудование и каналы связи находятся под единым контролем в доверенной зоне. Кроме того, все приложения также являются доверенными и предоставляются (разрабатываются) тем же провайдером. Такой вариант характерен для развертывания ПКС в едином центре, а более сложные режимы «Б» (наличие вторых и третьих участников разработки приложений, территориальная распределенность системы) и «В» (виртуализация сетевых функций) требуют отдельного рассмотрения.

Исходя из возможных угроз и практик по обеспечению безопасности контроллера, можно сформулировать общие *«функциональные требования»* безопасности, которые могут быть непосредственно не связаны с проектированием и разработкой контроллера, но они важны для его среды, эксплуатации или управления. В формате профиля защиты ГОСТ 15408 это семейства и компоненты требований:

Таблица 1. Общие функциональные требования

Table 1. General functional requirements

Семейство требований **Requirement family**	**Компоненты требований** **Requirement components**
Проверка IP	
Аутентификация пользователя	
Управление учетными записями	
Целостность и согласованность оборудования	
Безопасность гипервизора	
Проверка целостности ПО	
Целостность передаваемых данных	
Функция журнала регистрации	Устойчивость функций Защита доступа к журналам Защита модификации от журнала
Защита конфиденциальности передаваемых данных	
Скрытие отображения пароля и ключей	
Разделение разных типов трафика	
Безопасность виртуальных машин	
Закрытие неиспользуемых служб	
Безопасность физического хоста	
Функция Anti-DoS:	Анти-DoS от исчерпания ресурсов, вычислительной мощности.
Разрешение на использование системных функций	
Разрешение интерфейса для третьих лиц (разработчиков ПО)	
Безопасность хостовой ОС	

Общие *«функциональные требования»* безопасности являются развитием требований к сетевым устройствам и коммуникациям, которые должны использовать-

ся для обеспечения безопасности управляющего контура ПКС. Контроллер ПКС представляет собой сетевую операционную систему, но он оперирует сетевыми сущностями, отличными от объектов операционных систем. По сути он представляет собой реализованную на основе операционной системы АСУ по управлению сетью. И несмотря на то что ряд функций безопасности контроллера ПКС может обеспечиваться функциональностью операционной системы (соответствующего класса защиты), архитектура ПКС выдвигает ряд специфических функциональных требований безопасности:

Таблица 2. Специальные функциональные требования

Table 2. Special functional requirements

Семейство требований **Requirement family**	**Компоненты требований** **Requirement components**
Аутентификация на интерфейсах контроллеров SDN	
Защита данных конфигурации и резервных копий от модификации	
Управление доступом к критической информации	
Скрытие отображения пароля и ключа	
Изоляция приложения	
Функция Anti-DoS	Ограничение пересылки («шторма») IP-пакетов в контроллер от коммутаторов Контроль доступа к таблицам потоков Мониторинг трафика интерфейсов приложений и сетевых устройств и блокировка DoS-атак Ограничение ресурсов для приложений – Анти-DoS от чрезмерного потребления ресурсов
Контроль за привилегиями приложений	
Политика разрешения конфликтов (создания правил потоков, доступа к информации и т.п.) приложений	

Изменяющийся характер конфигураций и связей ПКС требует определения и отражения в виде *«политик»* и *«предположений»* безопасного начального состояния и сохранения заданного уровня безопасности в процессе изменений. Кроме того, такая изменчивость может приводить к конфликту правил, реализуемых различными приложениями. Это вызывает необходимость включения в состав *«функциональных требований»* спецификаций для процедур разрешения таких конфликтов.

Авторы сознательно не рассматривали «требования доверия», поскольку факторы, определяющие эту категорию требований, выходят за рамки инфраструктурной архитектуры и определяются в основном критичностью информационных активов.

Заключение

Таким образом, сформулирован базис для всех аспектов представления объекта и среды и их взаимодействия в контексте проблем безопасности. Это позволило подготовить спецификации конкретных угроз, предположений и политик, объединенных общим целями безопасности, как для объекта (контроллера ПКС), так и для среды его функционирования, и приступить к формированию функциональных требований безопасности. Дифференциация уровней, определяющих состав функциональных требований безопасности, предполагает несколько классов защиты. При разработке профиля защиты контроллера ПКС было принято, что рассматривается класс безопасности с минимальным составом функциональных требований безопасности, а для конкретного использования класс может быть уточнен. В рамках этих условий в МТУСИ был разработан проект профиля защиты контроллера программно-конфигурируемых сетей типа «А» пятого класса защиты (ИТ.КПКС.А5.ПЗ).

Список литературы / References

[1] *ISO/IEC 15408-1:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*, https://www.iso.org/standard/40612.html.

[2] Anwer B., et al., “A Slick Control Plane for Network Middleboxes”, *Open Networking Summit*, 2013, http://nextstep-esolutions.com/Clients/ONS2.0/pdf/2013/researchtrack/posterpapers/final/ons2013-final51.pdf.

[3] Fayazbakhsh S., et al., “FlowTags: Enforcing Network-Wide Policies in the Presence of Dynamic Middlebox Actions”, *HotSDN’13*, ACM, 2013, http://www.cs.columbia.edu/~lierranli/coms6998-8SDNFall2013/papers/Flowtags-HotSDN2013.pdf.

[4] Qazi Z.A., et al., “SIMPLE-fying Middlebox Policy Enforcement Using SDN”, *SIGCOMM*, ACM, 2013.

[5] *ONF Threat Analysis for the SDN Architecture. Version 1.0*, TR-530, July 2016, https://www.opennetworking.org/wp-content/Threat_Analysis_for_the_SDN_Architecture.pdf.

[6] Pilyugin P., Smeliansky R., “Modern security issues in SDN”, 2-nd International Conference on Information Technologies, Systems and Networks. ITSN-2017 (Chisinau, Republic of Moldova, 17 – 18 October 2017).

[7] *ONF Security Foundation Requirements for SDN Controllers. Version 1.0*, TR-529, July 2016, https://www.opennetworking.org/wp-content/Security_Foundation_Requirements_for_SDN_Controllers.pdf.

Petukhov A. N., Pilyugin P. L., "«Common Criteria» and Software Defined Network Security", *Modeling and Analysis of Information Systems*, **26**:1 (2019), 134–145.

DOI: 10.18255/1818-1015-2019-1-134-145

Abstract. «Common criteria» (ISO 15408) is a universally recognized and broadly applicable approach to information security solutions management and evaluation. «Common criteria» leans on developing a shared conceptual basis for key security solution modules including protection profiles and security targets. Conceptual basis development implies defining the following elements: security objectives and assumptions (for the environment and the object), threats and security policies, as well as functional and assurance requirements. The specifics of SDN (software defined network) security solutions is largely driven by fundamental architectural principles of SDN technology itself – primarily

by the separation of control and data flows, – and by conditions imposed by Open Flow protocol application. However, proactive (threats and policies), passive (objectives and assumptions) and reactive (requirements) aspects of security management remain highly relevant for this type of security solutions. This paper discusses the Common Criteria application specifics for assessing the SDN security and practical MTUCI (Moscow Technical University of Communications and Informatics) experience in the development of the protection profile. A new class of network attacks on SDN switches and controllers can involve either data or control components. In addition to traditional vulnerabilities, centralization of management functions paves way for new security threats by isolating controller activity and administrative message exchange. Therefore, identifying and analyzing threats, policies and requirements specific to SDN control module security becomes an emerging priority.

Keywords: security of software defined networks, general criteria, security profile

On the authors:
Andrey Petukhov, PhD, orcid.org/0000-0002-1427-2440
National Research University of Electronic Technology – MIET
Bld. 1, Shokin Square, Zelenograd, Moscow, Russia, 124498, e-mail: anpetukhov@yandex.ru

Paul Pilyugin, PhD, orcid.org/0000-0003-0011-7180
Lomonosov Moscow State University,
GSP-1, Leninskie Gory, Moscow, 119991, Russia, e-mail: ppl@mail.ru

Acknowledgments:
The work was supported by MTUCI (Moscow Technical University of Communications and Informatics) rectorate: Erokhin S., Leokhin Yu. and Mukhanov A., and with funding from the MTUCI, in the direction of «Security of critical information infrastructures».