Труды МАИ. 2022. № 123
Trudy MAI, 2022, no. 123

Научная статья
УДК 621.396
DOI: 10.34759/trd-2022-123-14

АНАЛИЗ ОПАСНЫХ СОБЫТИЙ И УЯЗВИМОСТЕЙ СУЩЕСТВУЮЩИХ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ 5G

Игорь Геннадьевич Бужин[1]✉, Вероника Михайловна Антонова[2], Юрий Борисович Миронов[3], Варвара Александровна Антонова[4]

[1,2,3,4]Московский технический университет связи и информатики, МТУСИ, Москва, Россия

[2] Институт радиотехники и электроники им. В.А. Котельникова РАН, Москва, Россия

[1]i.g.buzhin@mtuci.ru✉

[2]xarti@mail.ru

[3]i.b.mironov@mtuci.ru

[4]varvara_zi@mail.ru

Аннотация. В статье проанализированы опасные события и уязвимости существующих транспортных сетей связи 5G; выявлены актуальные угрозы безопасности информации для 5G/SDN/NFV; приведены рекомендации операторам сетей 5G для решения потенциальных проблем безопасности сетей 5G.

***Ключевые слова*:** 5G, угрозы, уязвимости, УБИ, модель угроз, сети передачи данных.

Для цитирования: Бужин И.Г., Антонова В.М., Миронов Ю.Б., Антонова В.А. Анализ опасных событий и уязвимостей существующих транспортных сетей связи 5G // Труды МАИ. 2022. № 123. DOI: 10.34759/trd-2022-123-14

ANALYSIS OF HAZARDOUS EVENTS AND VULNERABILITIES OF 5G TRANSPORT COMMUNICATION NETWORKS

Igor G. Buzhin[1]✉, Veronika M. Antonova[2],

Yuri B. Mironov[3], Varvara A. Antonova[4]

[1,2,3,4]Moscow technical university of communications and informatics,

Moscow, Russia

[2] Kotel'nikov institute of radio engineering and electronics of RAS, Moscow, Russia

[1]i.g.buzhin@mtuci.ru✉

[2]xarti@mail.ru

[3]i.b.mironov@mtuci.ru

[4]varvara_zi@mail.ru

Abstract. Being compared to the 3G and 4G, the 5G network offers significant increase in data-transmission rate, delay reduction and high-reliability connection. These advantages will allow organizations to operate more effectively, as well as render services quicker, enhancing their quality. Data throughput of the fifth-generation networks is higher, thus, connection of comparatively greater number of users and devices is possible.

The most serious safety hazards facing consumers and enterprises in the 5G networks are as follows:

1. Significantly larger surface of attack.

2. Severe aftermath caused by cyber-attacks.

3. A potential for more aggressive spying.

4. Subscribers' activity monitoring attacks.

5. Dangerous DDoS attacks.

Let us consider the 5G/SDN/NFV possible vulnerabilities classification. Vulnerabilities occurring due to the insufficient organization of information technical protecting from the unauthorized access and technical channels of information leakage are beyond the scope of the system under consideration. In general, the SDN/NFV security ensuring issues are considered in [1, 2, 3, 4, 5, 6]. They are:

• Software vulnerabilities.

• Vulnerabilities caused by the presence of a software-hardware bug in the 5G/SDN/NFV equipment [7].

• Vulnerabilities of network interaction protocols implementation and data transfer channels (IP, OpenFlow, etc.) [7].

• Vulnerabilities of the information security tools (the ones in the form of PNF, VNF), software and hardware.

Let us adduce a possible information security threats (IST) classification [7]:

• The IST by the information type being processed in the system:

  – voice information;

  – information processed by technical means of information processing;

• The IST by type of possible sources:

  – an external intruder;

  – an internal intruder;

  – malware;

  – a hardware bug (embedded or stand-alone) (not considered in this model).

• The IST by type of the information security property that is violated:

– information confidentiality (leakage, interception, capture, copying, theft, provisioning, distribution);

– information integrity (loss, theft, destruction, unauthorized changes);

– information availability (blocking);

– accountability of processes;

– repudiation of information or actions.

• The IST by the system type: since the 5G/SDN/NFV refers to the class of distributed 5G/ SDN/ NFV connected to the international information exchange network, threats specific to this type of system are considered.

• The IST by type of implementation:

– implemented through special impacts (of mechanical, chemical, acoustic, biological, radiation, thermal, electromagnetic nature) (not considered in this model);

– implemented through leakages from technical channels (not covered in this model);

– implemented through unauthorized access to the 5G/SDN/NFV;

• IST by type of the vulnerability utilized:

– related to the use of software vulnerabilities (hypervisors, virtual features);

– associated with application vulnerabilities;

– implemented through hardware bugs (not covered in this model);

– related to vulnerabilities in network protocols and communication channels (IP, Openflow);

– the ones the implementation of which is possible due to the vulnerabilities related to the gaps in the technical protection of information from unauthorized access (not covered in this model);

– implemented through vulnerabilities associated with the technical channels of information leakage (not considered in this model) [10];

– related to the vulnerabilities of information security tools;

– man-made threats.

• IST by type of the object being affected:

– information processed at the automated workstations of the system administrator and user;

– information processed in peripheral processing equipment (printers, plotters, remote monitors, video projectors, sound reproduction equipment, etc.) (not covered in this model);

– information transmitted through communications channels (while transmitted, while processed);

– information processed within the 5G/SDN/NFV virtual infrastructure and that includes storage;

– applications;

– software providing the 5G/SDN/NFV operation (SDN/NFV units, virtualization tools).

Considering the possible consequences of the IST implementation, we should focus on violating the key properties of information to ensure its security: confidentiality, integrity, availability, accountability, nonrepudiation.

Keywords: 5G, threats, vulnerabilities, threat model, data networks.

For citation: Buzhin I.G., Antonova V.M., Mironov Yu.B., Antonova V.A. Analysis of hazardous events and vulnerabilities of 5G transport communication networks. *Trudy MAI*, 2022, no.123. DOI: 10.34759/trd-2022-123-14

Введение

Сети 5 поколения состоят из основных элементов:

- абонентское оборудование с USIM-картами;
- сети радиодоступа (RAN) и поддержки пакетов backhaul и fronthaul1;
- ядра сети (5GC).

По сравнению с сетями 3G и 4G, 5G предлагает значительное увеличение скорости передачи данных, сокращение задержки и соединения высокой надежности. Эти преимущества дадут возможность организациям работать эффективнее, а также предоставлять услуги быстрее, делая их качественнее. Пропускная способность сетей 5 поколения выше, таким образом, возможно подключение сравнительно большого числа пользователей и устройств.

Рассмотрим наиболее опасные угрозы безопасности, с которыми могут столкнуться потребители и организации в сетях 5 поколения:

1. Расширенная поверхность атаки. Возможность подключения сравнительно большого количества устройств Интернета вещей влечет за собой большее количество точек входа для целевых атак. Каждый день увеличивается количество умных устройств, соответственно каждое из них может стать потенциальной целью злоумышленников.

2. Неблагоприятные последствия кибератак. Организации и инфраструктуры будут значительно зависеть от сетей 5 поколения: «умный» транспорт, оборудование заводов, «умные» фермы и т.д. Увеличение количества взаимосвязанных устройств и инфраструктур приведет к тому, что нарушение безопасности в одной из областей может привести к критическим последствиям.

3. Вероятность агрессивного шпионажа. Расширение возможностей устройств технологии Интернета вещей дает возможность злоумышленникам вести агрессивный шпионаж за потребителями: камеры и аудио возможности оборудования могут использоваться злоумышленниками с целью получения видео и аудио информации пользователей.

4. Мониторинг активности абонентов. Уязвимости всех протоколов AKE, в том числе протоколов сетей 5 поколения, могут быть использованы для реализации угроз, связанных с мониторингом активности абонентов. Для реализации атак «мониторинга активности абонентов» используются поддельные атаки на базовые станции, нацеленные на уязвимые протоколы AKE и уязвимость в шифровании SQNs.

5. DDoS-атаки. Как отмечалось ранее сети 5 поколения предполагают сокращение задержки, таким образом злоумышленники могут производить атаки значительно быстрее - в считанные секунды, а не минуты. Увеличение количества устройств Интернета вещей приведет к увеличению частоты атак.

Сети 5 поколения должна соответствовать архитектурным требованиям высокого уровня:

- поддержка большого числа выделенных сетей;
- различные требования к сети при предоставлении услуг и приложений;
- автоматическое конфигурирование и мониторинг предоставляемых сервисов и виртуальных и физических ресурсов;
- ускоренный ввод новых услуг и сервисов;
- гарантированное качество сопровождения и обслуживания.

Вследствие этого, сети 5 поколения предполагают абсолютное автоматическое конфигурирование новых услуг и сервисов, моментальное выделение необходимых сетевых ресурсов и обеспечение качественного обслуживания. Обеспечение перечисленных выше требований сетей 5G может быть достигнуто внедрением в транспортные сети 5G технологий SDN/NFV.

Модель угроз безопасности сетей 5G

Основными источниками угроз безопасности и факторами, влияющими на работоспособность транспортной сети 5G на базе технологии SDN/NFV являются:

- протоколы управления сетевыми устройствами. Такие протоколы ПКС, как OpenFlow, NETCONF, PCEP, OpFlex, OF-Config и другие позволяют конфигурировать и гибко управлять сетевыми устройствами;
- открытые программные интерфейсы: «южный» интерфейс (между уровнем управления и уровнем данных), «северный» интерфейс (между уровнем приложений и уровнем управления), «восточный» и «западный» интерфейсы в контуре управления, которые позволяют организовать распределенный контур управления;
- технология виртуализации сетевых функций (NFV). NFV виртуализирует сетевые сервисы, помогая быть аппаратно независимыми. Например, виртуализация позволяет развернуть виртуальную сеть из логических коммутаторов ПКС через общую аппаратную платформу.

Рассмотрим возможную классификацию уязвимостей 5G/SDN/NFV. Уязвимости, возникающие в следствие недостаточной организации технической защиты информации от НСД и технических каналов утечки информации, находятся

за границами рассматриваемой системы. В целом, вопросы обеспечения безопасности SDN/NFV рассмотрены в [1, 2, 3, 4, 5, 6].

1) Уязвимости ПО:

- микропрограмм, прошивок (физического оборудования, PNF);
- драйверов аппаратных средств (физического оборудования, PNF);
- ОС (ОС АРМ, платформы виртуализации);
- гипервизора;
- VNF и прочих виртуализированных функций;
- ПО автоматизированного рабочего места пользователя или администратора.

2) Уязвимости, связанные с наличием программно-аппаратной закладки в технических средствах 5G/SDN/NFV [7].

3) Уязвимости, связанные с протоколами сетевого взаимодействия и каналов передачи данных (IP, OpenFlow и т.д.) [7].

4) Уязвимости СЗИ (СЗИ в виде PNF, VNF), программно-аппаратных средств.

Уязвимости возникают в следствие [7]:

- ошибок проектирования и разработки ПО, ПАО (например, VNF, прошивок и т.д., платформ виртуализации, сетевых функций);
- преднамеренного внесения уязвимостей при проектировании и разработке ПО, ПАО (например, VNF, прошивок и т.д., платформ виртуализации, сетевых функций);
- неверных настроек ПО (VNF, прошивок, сетевых функций, приложений);

- неправомерного изменения режимов работы АО, гипервизора, приложений и т.д.;
- несанкционированного использования неучтенного ПО - приложений, VNF и т.д.;
- внедрения вредоносного ПО;
- действий неумышленного характера пользователей или администраторов, которые могут привести к возникновению уязвимостей;
- сбоев в функционировании аппаратного, программного и программно-аппаратного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Некоторыми уязвимостями SDN и протокола OpenFlow являются:

- централизация управления сетью;
- программная реализации на контроллере SDN механизмов защиты от типовых атак, связанных с подделкой адресов отправителя, на канальный и сетевой уровни модели OSI: ARP spoofing, DHCP snooping, IP spoofing и др.;
- необходимость отправки пакетов контроллеру для первичной обработки и выработки правил маршрутизации;
- применение агрегации (объединения) потоков в протоколе OpenFlow. В целях уменьшения количества памяти, выделяемых для хранения правил в таблице адресации, в протоколе OpenFlow реализована поддержка агрегации

потоков, в рамках которой часть правил может быть объединена по общим характеристикам (один и тот же порт получателя, адрес получателя и т.п.).

Цель определения угроз безопасности информации (УБИ) – определение существует ли возможность нарушения ключевых принципов информационной безопасности: конфиденциальности, целостности, доступности, подотчетности, невозможности от отказа авторства информации, содержащейся в 5G/SDN/NFV, или невозможности от отказа авторства действий в 5G/SDN/NFV, и возможен ли неприемлемый ущерб любого вида при нарушении хотя бы одного свойства безопасности [8].

Источники антропогенных угроз 5G/SDN/NFV [8]:

- физические лица, осуществляющие действия (преднамеренные) с целью доступа к 5G/SDN/NFV или нарушения функционирования 5G/SDN/NFV или инфраструктуры (преднамеренные УБИ);
- лица, имеющие доступ к 5G/SDN/NFV, действия которых (не преднамеренные) могут привести к нарушению ИБ (непреднамеренные УБИ).

Источники техногенных угроз 5G/SDN/NFV [8]:

- неисправность аппаратного и программного обеспечения, а также физических каналов связи;
- отсутствие подсистемы резервного копирования программного обеспечения и резервирования аппаратных средств;
- отсутствие резервирования инженерных систем: электроснабжение, кондиционирование, охрана и т.д.;

- некачественное сопровождение, обслуживание и ремонт аппаратного и программного обеспечения.

В модель угроз включаются только актуальные УБИ, подлежат нейтрализации те УБИ, актуальность которых заключается в возможности реализации угрозы нарушителем с заданным потенциалом и наличии ущерба от реализации угрозы.

Перечень угроз безопасности формируется с использованием Банка данных угроз безопасности информации ФСТЭК России [9], размещенном на официальном сайте, с учетом особенностей 5G/SDN/NFV. При этом в данной модели угроз исключены неактуальные угрозы или угрозы, выходящие за рамки рассматриваемой системы 5G/SDN/NFV:

- угрозы для грид-систем,
- угрозы для суперкомпьютеров,
- угрозы для систем хранения больших данных.

УБИ является актуальной для 5G/SDN/NFV с заданной структурой и характеристиками, если существует возможность реализации УБИ нарушителем с соответствующим потенциалом, а реализация УБИ приведет к неприемлемому ущербу от нарушения свойств безопасности информации [8].

Чтобы определить возможность реализации УБИ, следует оценить уровень защищенности 5G/SDN/NFV, а также потенциал нарушителя, требуемого для реализации УБИ.

На этапе оценки 5G/SDN/NFV систем при определении возможности реализации УБИ, согласно [8], следует руководствоваться уровнем проектной защищенности 5G/SDN/NFV. Анализируя показатели [8], следует прийти к выводу,

что 5G/SDN/NFV на этапе разработки является системой с низкой проектной защищенностью.

Таким образом, учитывая низкий уровень проектной защищенности и высокий потенциал нарушителя, следует всем возможным УБИ 5G/SDN/NFV предварительно присвоить высокий уровень возможности реализации.

Оценивая степень ущерба от реализации УБИ, следует прийти к выводу, что в результате нарушения одного из ключевых свойств безопасности информации возможны существенные негативные последствия для 5G/SDN/NFV. То есть 5G/SDN/NFV и/или администратор (пользователь) не будут иметь возможности выполнять возложенные на них функции. Таким образом, степень ущерба – высокая.

Учитывая высокий уровень возможности реализации УБИ, высокую возможную степень ущерба от реализации УБИ, следует сделать вывод об актуальности многих УБИ для 5G/SDN/NFV.

Учитывая то, что каждую УБИ оценить отдельно возможно только на этапе создания конкретной 5G/SDN/NFV системы, то многие УБИ следует считать актуальными.

Приведем классификацию возможных УБИ [7]:

1) УБИ по виду информации, обрабатываемой в системе:
   - речевой информации;
   - информации, обрабатываемой техническими средства обработки информации.
2) УБИ по видам возможных источников:
   - внешний нарушитель;

- внутренний нарушитель;
- вредоносная программа;
- аппаратная закладка (встроенная либо автономная) (не рассматривается в данной модели).

3) УБИ по нарушаемому свойству информационной безопасности:
   - конфиденциальности (утечка, перехват, съем, копирование, хищение, предоставление, распространение) информации;
   - целостности (утрата, кража, уничтожение, несанкционированное изменение) информации,
   - доступности (блокирование) информации;
   - подотчетности действий;
   - отказа от авторства информации, действий.
4) УБИ по типу системы - поскольку 5G/SDN/NFV относится к классу распределенной 5G/SDN/NFV, подключенной к сети международного информационного обмена, то рассматриваются угрозы, характерные для систем такого типа,
5) УБИ по способу реализации:
   - реализуемые за счет специальных воздействий (механического, химического, акустического, биологического, радиационного, термического, электромагнитного характера) (не рассматривается в данной модели);
   - реализуемые за счет утечки по техническим каналам (настоящая модель не охватывает);

- реализуемые за счет НСД к 5G/SDN/NFV.

6) УБИ типу по задействованной уязвимости:

- связанные с использованием уязвимости программного обеспечения (гипервизоров, виртуальных функций);
- связанные с уязвимостями приложений;
- реализуемые через аппаратные закладки (настоящая модель не охватывает);
- связанные с уязвимостями сетевых протоколов и каналов связи (IP, Openflow);
- реализация которых возможна ввиду уязвимостей, связанных с недостатками технической защиты информации от НСД (настоящая модель не охватывает);
- реализуемые через уязвимости, связанными с наличием технических каналов утечки информации (не рассматривается в данной модели) [10];
- связанные с уязвимостями СЗИ,
- техногенные угрозы.

7) УБИ по объекту воздействия:

- информации, обрабатываемой на автоматизированных рабочих местах администратора и пользователя системы;
- информации, обрабатываемой в периферийных средствах обработки (принтерах, плоттерах, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.) (настоящая модель не охватывает);

- информации, передающейся по каналам связи (при передаче, при обработке);
- информации, обрабатываемой внутри виртуальной инфраструктуры 5G/SDN/NFV, в том числе при хранении;
- приложения;
- ПО, обеспечивающему функционирование 5G/SDN/NFV (блоки SDN/NFV, средства виртуализации).

Анализируя международные спецификации, иностранную литературу, следует сделать вывод о наиболее актуальных УБИ для 5G/SDN/NFV. Особенностью концепции SDN/NFV является то, что значительная часть инфраструктуры передачи данных, которая в классической сети представляет собой программно-аппаратный комплекс (ПАК), в SDN/NFV виртуализируется на серверах, таким образом порождая угрозы, характерные для ПО:

- перехват информации с анализом трафика;
- внедрение вредоносных программ, приложений, VNF из репозитория;
- выявление паролей;
- конфликт правил потока (Flow rules confliction) - конфликт может возникнуть вследствие того, что протоколы 5G/SDN/NFV (OpenFlow) не различают приложения, создающие запись таблицы потоков коммутаторов SDN, с другими приложениями, которые создали запись ранее, угроза приводит к созданию путей трафика в обход средств защиты в сети (при скомпрометированном приложении);

- создание ложного маршрута несанкционированным изменением таблиц потоков;
- несанкционированное перенаправление потока данных;
- отказ в обслуживании коммутатора – отказ в обслуживании на коммутатор может быть осуществлен генерацией неизвестного для коммутатора трафика; коммутатор будет обращаться к контроллеру для определения правила потока нового трафика, что при большом объеме запросов приведет к исчерпанию ресурсов канала связи между коммутатором и контроллером;
- отказ в обслуживании контроллера – быть осуществлен генерацией неизвестного для коммутатора трафика; коммутатор будет обращаться к контроллеру для определения правила потока нового трафика, что при большом объеме запросов приведет к исчерпанию вычислительных ресурсов контроллера;
- переполнение журналов регистрации событий;
- переполнение счетчиков данных;
- переполнение таблицы адресации потоков коммутатора;
- подмена доверенного объекта (в т.ч. коммутатора, контроллера, приложения и прочего);
- получение НСД к каналу управления между коммутатором и контролером (при коммутаторе в виде PNF);
- получение НСД к 5G/SDN/NFV и ее отдельным элементам;
- потеря коммутатором связи с контроллером;

- сканирования, направленные на определение топологии сети, открытых портов и служб, открытых соединений и др.;
- создание несанкционированных правил потоков (Fake flow rule insertion);
- угроза нарушения доступности физического оборудования, на котором размещен контроллер;
- угроза нарушения доступности физического оборудования, на котором размещен коммутатор либо нарушение работоспособности самого коммутатора при его аппаратном исполнении;
- угрозы, характерные для программного обеспечения и средств виртуализации;
- удаленный запуск приложений.

Характерные техногенные угрозы:

- отказы и сбои станций управления и мониторинга;
- отказы и сбои АРМ;
- непреднамеренная ошибка маршрутизации;
- отказы и сбои серверного оборудования;
- отказы и сбои дисковых массивов;
- отказы и сбои сетевого оборудования;
- пропадание каналов связи;
- отказ системы энергоснабжения;
- отказ системы кондиционирования;
- пожар;
- затопление;

- стихийные бедствия.

Заключение

Рассматривая возможные последствия реализации УБИ, следует ориентироваться на нарушение ключевых свойств информации в рамках обеспечения ее безопасности: конфиденциальности, целостности, доступности, подотчетности, невозможности отказа от авторства. Принимая во внимание проблемы безопасности сетей предыдущего поколения и рассмотренные угрозы и уязвимости сетей 5G, можно сделать вывод, что операторы должны использовать комплексный подход к защите сети, проводить аудит безопасности и постоянно совершенствовать систему безопасности. Необходимо проводить анализ всей сигнальной информации, пересекающей границу их домашней сети с целью блокировки неразрешенного трафика. Периодическое проведение аудита безопасности позволит выявить изменения в безопасности сети и своевременно принять контрмеры. Регулярное изучение и внедрение новых рекомендаций по защите сетей 5G должно позволит обеспечивать безопасность на должном уровне.

СПИСОК ИСТОЧНИКОВ

1. Shang Gao, Zecheng Li, Bin Xiao, Guiyi Wei. Security Threats in the Data Plane of Software-Defined Networks // IEEE Network, 2018, pp. 1-6. DOI: 10.1109/MNET.2018.1700283

2. Casado M., Garfinkel T., Akella A., Freedman M.J., Boneh D., McKeown N., Shenker S. SANE: A protection architecture for enterprise networks // USENIX Security Symposium, 2006.

3. Scott-Hayward S., Natarajan S., Sezer S. A Survey of Security in Software Defined Networks // IEEE Communications Surveys and Tutorials, 2016, vol. 18 (1), pp. 623-654. DOI: 10.1109/COMST.2015.2453114

4. Захаров А.А., Попов Е.Ф., Фучко М.М. Аспекты информационной безопасности архитектуры SDN // Вестник СибГУТИ. 2016. № 1 (33). С. 83-92.

5. Ефимушкин В.А., Ледовских Т.В., Корабельников Д.М., Языков Д.Н. Обзор решений SDN/NFV зарубежных производителей // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 8. С. 5-13.

6. Волков С.С., Курочкин И.И. Применение методов машинного обучения в SDN в задачах обнаружения вторжений // International Journal of Open Information Technologies. 2019. Т. 7. № 11. С. 49-58.

7. Агеев С.А. и др. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2011. № 1. С. 50-57.

8. Якупов Р.Р. и др. Методика определения угроз безопасности информации в ИС. // Свидетельство о государственной регистрации программы для ЭВМ. № RU 2017612328, 20.02.2017.

9. Безродных О.А. Систематизация угроз безопасности информации для упрощения построения модели угроз // StudNet. 2021. Т. 4. № 4. URL:

https://cyberleninka.ru/article/n/sistematizatsiya-ugroz-bezopasnosti-informatsii-dlya-uproscheniya-postroeniya-modeli-ugroz?

10. Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных сетях // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2013. Т. 11. №. 2. С. 55-72.

11. Бахтин А.А., Волков А.С., Солодков А.В., Баскаков А.Е. Разработка модели сегмента сети SDN для стандарта 5G // Труды МАИ. 2021. № 117. URL: https://trudymai.ru/published.php?ID=122307. DOI: 10.34759/trd-2021-117-07

12. Волков А.С., Баскаков А.Е. Разработка процедуры двунаправленного поиска для решения задачи маршрутизации в транспортных программно-конфигурируемых сетей // Труды МАИ. 2021. № 118. URL: https://trudymai.ru/published.php?ID=158240. DOI: 10.34759/trd-2021-118-07

13. Курочкин И.И., Гуменный Д.Г. Безопасность сетей SDN. Классификация атак // Современные информационные технологии и ИТ-образование. 2015. Т. 11. № 2. С. 381-383.

14. Principles and Practices for Securing Software-Defined Networks. ONF TR-511 Open Networking Foundation, 2015. URL: https://pdfslide.net/documents/principles-and-practices-for-securing-software-defined-networks.html

15. Антонов А.И., Киреева Н.В. Обеспечение информационной безопасности в сетях 5G // III Научный форум телекоммуникации: теория и технологии ТТТ-2019 (Казань, 18–22 ноября 2019): сборник трудов. – Казань, Казанский государственный технический университет им. А.Н. Туполева, 2019. С. 567-568.

16. Ji X. et al. Overview of 5G security technology // Science China Information Sciences, 2018, vol. 61, no. 8, pp. 1-25. DOI:10.1007/s11432-017-9426-4

17. Chamola V. et al. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography // Computer Communications, 2021, vol. 176, pp. 99-118. DOI:10.1016/j.comcom.2021.05.019

18. Khan J.A., Chowdhury M.M. Security Analysis of 5G Network // 2021 IEEE International Conference on Electro Information Technology (EIT), 2021, pp. 001-006.

19. Soldani D. 5G and the Future of Security in ICT // 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, 2019, pp. 1-8. DOI:10.1109/ITNAC46935.2019.9078011

20. Prasad A.R. et al. 3GPP 5G security // Journal of ICT Standardization, 2018, vol. 6, no. 1, pp. 137-158. DOI:10.13052/jicts2245-800X.619

21. Salman O. et al. Multi-level security for the 5G/IoT ubiquitous network // 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), IEEE, 2017, pp. 188-193. DOI:10.1109/FMEC.2017.7946429

References

1. Shang Gao, Zecheng Li, Bin Xiao, Guiyi Wei. Security Threats in the Data Plane of Software-Defined Networks, *IEEE Network,* 2018, pp. 1-6. DOI: 10.1109/MNET.2018.1700283

2. Casado M., Garfinkel T., Akella A., Freedman M.J., Boneh D., McKeown N., Shenker S. SANE: A protection architecture for enterprise networks, *USENIX Security Symposium,* 2006.

3. Scott-Hayward S., Natarajan S., Sezer S. A Survey of Security in Software Defined Networks, *IEEE Communications Surveys and Tutorials*, 2016, vol. 18 (1), pp. 623-654. DOI: 10.1109/COMST.2015.2453114

4. Zakharov A.A., Popov E.F., Fuchko M.M. *Vestnik SibGUTI*, 2016, no. 1 (33), pp. 83-92.

5. Efimushkin V.A., Ledovskikh T.V., Korabel'nikov D.M., Yazykov D.N. *T-Comm: Telekommunikatsii i transport*, 2015, vol. 9, no. 8, pp. 5-13.

6. Volkov S.S., Kurochkin I.I. *International Journal of Open Information Technologies*, 2019, vol. 7, no. 11, pp. 49-58.

7. Ageev S.A. et al. *Avtomatizatsiya protsessov upravleniya*, 2011, no 1, pp. 50-57.

8. Yakupov R.R. et al. *Svidetel'stvo o gosudarstvennoi registratsii programmy dlya EVM. RU 2017612328*, 20.02.2017.

9. Bezrodnykh O.A. *StudNet,* 2021, vol. 4, no. 4. URL: https://cyberleninka.ru/article/n/sistematizatsiya-ugroz-bezopasnosti-informatsii-dlya-uproscheniya-postroeniya-modeli-ugroz?

10. Mukhanova A.A., Revnivykh A.V., Fedotov A.M. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii*, 2013, vol. 11, no. 2, pp. 55-72.

11. Bakhtin A.A., Volkov A.S., Solodkov A.V., Baskakov A.E. *Trudy MAI*, 2021, no. 117. URL: https://trudymai.ru/eng/published.php?ID=122307. DOI: 10.34759/trd-2021-117-07

12. Volkov A.S., Baskakov A.E. *Trudy MAI*, 2021, no. 118. URL: https://trudymai.ru/eng/published.php?ID=158240. DOI: 10.34759/trd-2021-118-07

13. Kurochkin I.I., Gumennyi D.G. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2015, vol. 11, no. 2, pp. 381-383.

14. *Principles and Practices for Securing Software-Defined Networks. ONF TR-511 Open Networking Foundation*, 2015. URL: https://pdfslide.net/documents/principles-and-practices-for-securing-software-defined-networks.html

15. Antonov A.I., Kireeva N.V. *III Nauchnyi forum telekommunikatsii: teoriya i tekhnologii TTT-2019, sbornik trudov*. Kazan', Kazanskii gosudarstvennyi tekhnicheskii universitet im. A.N. Tupoleva, 2019, pp. 567-568.

16. Ji X. et al. Overview of 5G security technology, *Science China Information Sciences,* 2018, vol. 61, no. 8, pp. 1-25. DOI:10.1007/s11432-017-9426-4

17. Chamola V. et al. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography, *Computer Communications,* 2021, vol. 176, pp. 99-118. DOI:10.1016/j.comcom.2021.05.019

18. Khan J.A., Chowdhury M.M. Security Analysis of 5G Network, *2021 IEEE International Conference on Electro Information Technology (EIT)*, 2021, pp. 001-006.

19. Soldani D. 5G and the Future of Security in ICT, *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, 2019, pp. 1-8. DOI:10.1109/ITNAC46935.2019.9078011

20. Prasad A.R. et al. 3GPP 5G security, *Journal of ICT Standardization,* 2018, vol. 6, no. 1, pp. 137-158. DOI:10.13052/jicts2245-800X.619

21. Salman O. et al. Multi-level security for the 5G/IoT ubiquitous network, *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, IEEE, 2017, pp. 188-193. DOI:10.1109/FMEC.2017.7946429

Статья поступила в редакцию 08.02.2022; одобрена после рецензирования 22.02.2022;

принята к публикации 20.04.2022.
The article was submitted on 08.02.2022; approved after reviewing on 22.02.2022; accepted for publication on 20.04.2022.