2. Jaber, G. Semantic information-centric networking naming schema / G. Jaber, N. V. Patsei, F. Rahal // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. - Минск : БГТУ, 2020. - № 1 (230). - С. 69-73.

3. Jaber G, Patsei N., Rahal F., Abboud A. Naming and Routing Scheme for Data Content Objects in Information-Centric Network // 2020 Open Conference of Electrical, Electronic and Information Sciences (eStream): Proceedings of the Conference : April 30, 2020, Vilnius, Lithuania, . IEEE -2020. P.93-97.

УДК 316.776; 004.056.5

Е.А. Гончар, маг.; Ю.А. Чистякова, преп.-стажер;
А.С. Пахолко, ассист. (БГТУ, г. Минск)

УГРОЗЫ И ПРОЕКТИРОВАНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ОРИЕНТИРОВАННЫХ СЕТЕЙ

Информационно-ориентированная сеть (*ICN – Information Centric Network*) – это новая сетевая парадигма, которая заменяет широко используемую, ориентированную на хост, в сетях связи (например Интернет, мобильные специальные сети) с информационно-ориентированной парадигмой, которая определяет приоритет доставки именованного контента, не обращая внимания на происхождение контента.

Парадигма *ICN* по своей сути поддерживает несколько функций безопасности и конфиденциальности, которые все еще недостаточно доступны в парадигме, ориентированной на хост.

Однако, *ICN* имеет несколько нерешенных проблем, связанных с безопасностью и конфиденциальностью, как старых, так и новых. На данный момент любой контент ориентирован на запросы пользователя, а, значит, должен обладать такими свойствами как: отказоустойчивость, быстрый доступ к контенту, высокая скорость доставки, а также безопасность конечного пользователя и контента потребляемого им. Использование архитектуры *ICN* сокращает время простоя системы из-за сбоев сервера, например, такие сбои были у пользователей *Netflix*, *Pinterest* и *Instagram* в США (22 октября 2012 г.). Таким образом, учитывая высокую скорость развития данного направления должны решаться важные задачи, связанные с безопасностью: обеспечение приватности и контроль доступа.

Учитывая то, что именованный контент может храниться где угодно в сети; каждый информационный объект должен быть уни-

кально адресован и запрошен. За последнее время было предложено несколько архитектур *ICN*, таких как: сеть именованных данных / контент-ориентированная сеть (*NDN – Named Data Networking*/ *CCN – Content-Centric Networking*), парадигма Интернет-маршрутизации с публикацией и подпиской (*PSIRP*), сетевая архитектура, ориентированная на данные (*DONA*), и сеть информации (*NetInf*). Хотя они различаются по своим деталям, у них есть несколько основных свойств: уникальное имя для контента, маршрутизация на основе имени, всеобъемлющее кэширование и гарантия целостности контента.

Согласно анализу работ [1] и [2] можно выделит следующие виды угроз для ICN:

1. DDoS/DoS;
2. атака с отравлением контентом;
3. атака с загрязнением кэша;
4. прочие.

DoS-атаки – это атаки, которые могут быть нацелены либо на промежуточные маршрутизаторы, либо на поставщиков контента. Самый простой тип атаки – обращение к контенту, которого нет многократно (рис. 1).

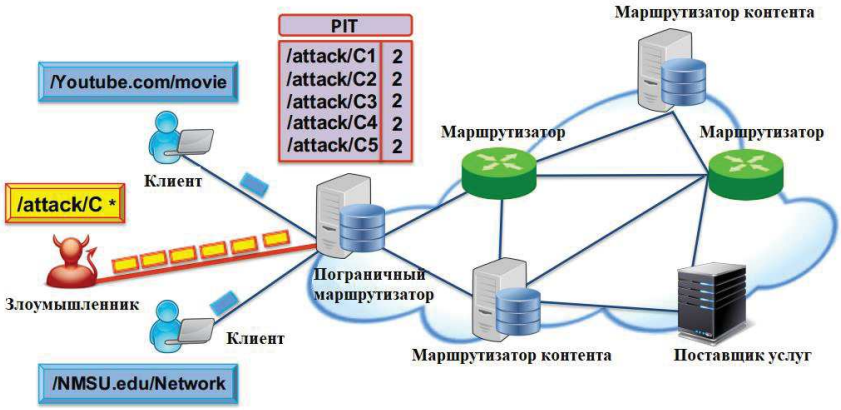

Рисунок 1 – Пример *DoS*-атаки на *ICN*

Для решения данной проблемы в [3] были предложены три подхода для борьбы с атаками в *NDN*. Они использовали небольшую модификацию хорошо известного алгоритма *Token Bucket*, в котором каждый маршрутизатор ограничивает количество ожидающих запросов “*интереса*” для каждого интерфейса, пропорционально его пропускной способности (произведение пропускной способности и задержки). Этот метод не очень эффективен, поскольку маршрутизатор может использовать всю пропускную способность канала для удовлетворения “*интересов”* злоумышленника, что снижает степень удовлетворения “*интересов”* законных клиентов. В предложенном подходе

маршрутизатор гарантирует, что пропускная способность исходящего канала равномерно распределяется между трафиком от всех входящих интерфейсов. Для этого в *PIT* (*Pending Interest Table*) добавлен новый столбец, в котором каждый запрос "*интереса"* обозначается как перенаправленный или находящийся в очереди. Маршрутизатор также поддерживает очередь для каждого входящего интерфейса. Это улучшение частично решает проблему, поскольку злоумышленник на одном интерфейсе не сможет использовать все ресурсы маршрутизатора. Однако, даже при таком подходе нет различия между злоумышленником и легитимным клиентом. "*Интересы"* как злоумышленников, так и законных клиентов ограничены по скорости, если они происходят на высокоскоростном интерфейсе.

Цель атаки с отравлением контента – заполнить кеш-память маршрутизатора недопустимым содержимым. Чтобы провести эту атаку, злоумышленник должен управлять одним или несколькими поставщиками контента или промежуточными маршрутизаторами, чтобы он мог внедрить свой собственный контент в сеть. Внедренный контент должен иметь действительное имя, соответствующее "*интересам"*, но поддельное информационное наполнение или недействительную подпись (рис. 2).

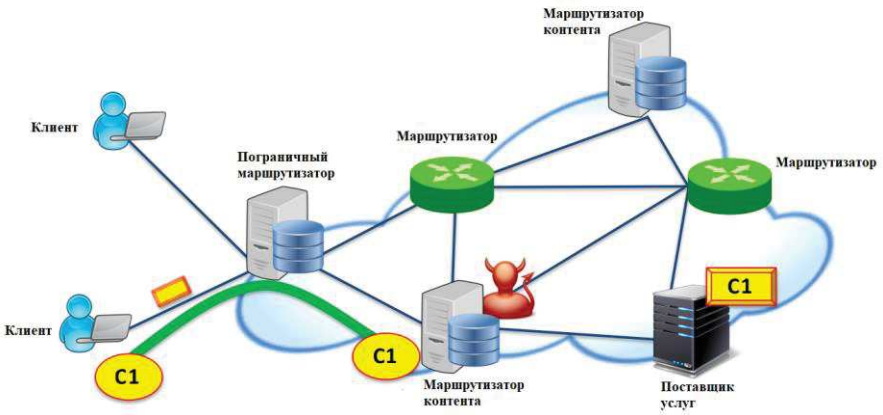

Рисунок 2 – Атака с отравлением контента

В [4] были впервые рассмотрены атаки отравления контента/кэша. В качестве меры противодействия было предложено использовать «самосертифицирующийся пакет интересов/данных» (*SCID* – (*Self-Certifying Interest/Data Packet*)), который помогает маршрутизаторам пересылки проверять полученные фрагменты контента. Перед отправкой запроса "*интереса"* клиент должен получить от поставщика контента хэш, имя и подпись желаемого фрагмента; эта информация затем присоединяется к "*интересам"*. При получении блока содержимого маршрутизатор может легко проверить его действительность, сравнив его хэш с хэшем из пула. Этот метод менее требовате-

лен к вычислениям, чем традиционная проверка подписи на основе *RSA*, однако он требует, чтобы клиент заранее получил хэш для каждого фрагмента/пакета данных. Необходимо, чтобы клиент запросил поставщика непосредственно перед запросом контента, что резко увеличивает задержку при извлечении контента и ограничивает масштабируемость.

В качестве альтернативного решения предлагается выполнить проверку подписи кэшированного содержимого маршрутизаторами. В базовой модели каждый маршрутизатор случайным образом выбирает блоки контента для проверки, проверяет подписи выбранных фрагментов и отбрасывает все поврежденные. Чтобы предотвратить избыточную проверку, маршрутизаторы совместно выбирают диапазон блоков контента для проверки. Чтобы уменьшить накладные расходы, предлагается использовать принятие решений с обратной связью с клиентом, при котором клиент может информировать свой граничный маршрутизатор о достоверности каждого фрагмента контента. Однако, этот тип обратной связи также может использоваться злоумышленниками для введения в заблуждение маршрутизаторов, сообщая о законных объектах контента как о поддельных, или наоборот.

Таким образом, был выполнен анализ ряда проблем и угроз в сетях, построенных в соответствии с архитектурой *ICN*, рассмотрены методы борьбы с основными угрозами и определены недостатки этих методов. Следует отметить, что методика обеспечения безопасности для архитектур *ICN* находится в стадии разработки.

ЛИТЕРАТУРА

1. C. Dannewitz. NetInf: An information-centric design for the future Internet. In 3rd GI/ITG KuVS Workshop on The Future Internet, 2009.

2. E. AbdAllah, H. Hassanein, and M. Zulkernine. A survey of security attacks in information-centric networking. IEEE Communications Surveys & Tutorials, 17:1441–1454, 2015.

3. A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and countermeasures in named data networking. In Proceedings of IFIP Networking Conference, pages 1–9. IEEE, 2013.

4. P. Gasti, G. Tsudik, E. Uzun, and L. Zhang. Dos and ddos in named data networking. In 22nd International Conference on Computer Communications and Networks (ICCCN), pages 1–7. IEEE, 2013.