3. Реверсинг малвари для начинающих : [сайт]. — URL: https://xakep.ru/2016/12/08/reversing-malware-tutorial-part1/ (дата обращения: 01.05.2022). — Текст : электронный.
4. Искусство антидетекта : [сайт]. — URL: https://www.securitylab.ru/analytics/485677.php (дата обращения: 01.04.2022). — Текст : электронный.
5. Что такое Emotet? : [сайт]. — URL : https://www.kaspersky.ru/resource-center/threats/what-is-emotet (дата обращения: 02.05.2022). — Текст : электронный.
6. Обзор правил YARA: изучение инструмента исследования вредоносного ПО : [сайт]. — URL: https://habr.com/ru/company/varonis/blog/584618/ (дата обращения: 21.04.2022). — Текст : электронный.

А. Р. Зиянгиров, А. М. Шабалин
Тюменский государственный университет, г. Тюмень

УДК 004.732

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ЦЕНТРАЛИЗОВАННОГО АДМИНИСТРИРОВАНИЯ БЕСПРОВОДНОЙ СЕТИ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ КОНТРОЛЛЕРА

Аннотация. *В статье рассматриваются способы организации и функционирования безопасного централизованного администрирования беспроводной сети предприятия с помощью контроллера. Результатом работы стала модель компьютерной сети предприятия с применением беспроводного контроллера с обеспечением необходимого уровня защиты беспроводных станций.*

Ключевые слова: *WLAN, Wi-Fi, беспроводной контроллер, CAPWAP, безопасность.*

Введение. В наши дни на многих предприятиях активно используются беспроводные сети, а значит существует потребность в том, чтобы обеспечить централизованное администрирование и безопасность таких подключений. Современные сети, построенные на независимых точках доступа, — это устаревшая немасштабируемая архитектура с ограниченным функционалом, поэтому все средние и крупные компании с развитием беспроводных систем переходят на

централизованное управление точками доступа из-за большого количества устройств и, соответственно, возникает спрос на управление безопасностью в таких сетях. Беспроводной контроллер — новое телекоммуникационное устройство, который обеспечивает централизованное управление точками доступа и их защищенность.

WLAN-устройства на данный момент более удобны в использовании, чем кабельные аналоги, что связано в первую очередь с доступностью оборудования, а также с широким списком устройств, которые поддерживают технологию Wi-Fi [1]. Безопасность WLAN-сетей за последние несколько лет стала качественнее в первую очередь из-за использования актуальных способов шифрования и централизованного контроля доступа. Сегодня безопасность WLAN может быть обеспечена с помощью функционала самих продуктов Wi-Fi, до такой степени, что беспроводная сеть будет даже более безопасной, чем кабельная [2]. Одна из главных рекомендаций по защите WLAN-сетей — использование продуктов с встроенными механизмами защиты [3].

Проблема исследования. Целью работы является организация безопасного централизованного администрирования беспроводной сети предприятия средствами WLAN-контроллера. Организация безопасного централизованного администрирования беспроводной сети предприятия — достаточно сложный и комплексный процесс, поэтому были выделены несколько задач:

1. Изучить технические особенности функционирования WLAN-контроллеров.
2. Сравнить современные протоколы управления беспроводными точками доступа.
3. Проанализировать современные методы обеспечения безопасности беспроводной сети средствами контроллера.
4. Смоделировать безопасную беспроводную сеть в программном эмуляторе.

Материалы и методы. Методами данного исследования стали: наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство Huawei eNSP 1.3.00.100 [4].

Результаты. WLAN-контроллер — это контроллер беспроводной локальной сети, объединяющий точки доступа, управляющий их работой, а также централизующий трафик. Беспроводной контроллер Huawei AC6605 — гибкое и многофункциональное решение для сетей среднего размера, которое предоставляет возможность управлять до 1024 точками доступа. Также данный контроллер позволяет использовать функцию Power over Ethernet, подавая питание на все свои 24 порта Gigabit Ethernet, в соответствии со стандартом IEEE 802.3af/at и поддерживая максимальную выходную мощность Power over Ethernet 380 Вт, что обеспечивает доступ для кабельных и беспроводных клиентов [5]. Отдельно стоит упомянуть высокую масштабируемость и гибкость в настройке управляемых им точек доступа. Данный контроллер эмулируется в программном средстве Huawei eNSP, что предопределило наш выбор для моделирования компьютерной сети.

Для связки контроллера доступа (access controller, AC) с точками доступа (access point, AP) будет использоваться централизованная архитектура управления точками доступа средствами беспроводного контроллера по протоколу CAPWAP (рис. 1), с помощью которого точка доступа автоматически обнаруживает контроллер, и он их аутентифицирует. Далее точки доступа получают конфигурацию, между ними устанавливается CAPWAP-туннель, использующийся для передачи контрольных пакетов.

Беспроводной контроллер отвечает за управление безопасным доступом к WLAN, пересылку данных и сбор статистики, настройку и мониторинг точек доступа, управление роумингом, мониторинг агентов управления сетью точек доступа и управление безопасностью. Точка доступа осуществляет шифрование и расшифровку кадров IEEE 802.11 и предоставляет функции физического уровня 802. 11, собирает статистику с радиоинтерфейса [6].

Режим организации сети, который будет реализован, это режим — Off-Path (рис. 2), позволяющий расширять беспроводную инфраструктуру. Для этого необходимо подключить контроллер к коммутатору агрегации или ядра. Данная организация беспроводной сети чаще используется в современных компаниях. В сети контроллер

управляет только точками доступа, а управляющий трафик инкапсулируется и передается в туннелях CAPWAP. Однако, трафик данных от пользователей может передаваться, как через контроллер по туннелям CAPWAP, так и передаваться в кампусную сеть напрямую и не проходить через сам контроллер точек доступа [7].

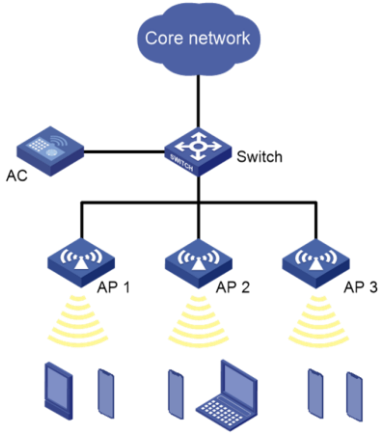

Рис. 1. Централизованная архитектура управления точками доступа

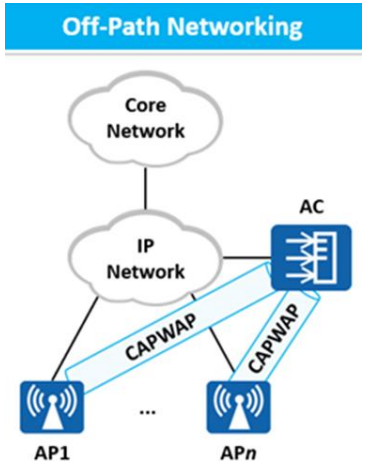

Рис. 2. Режим организации сети «Off-Path»

Протокол CAPWAP — это стандартный, совместимый сетевой протокол, который позволяет центральному контроллеру доступа беспроводной локальной сети управлять набором беспроводных точек доступа. Основан на проприетарном протоколе LWAPP от Cisco и на сегодняшний день является стандартом, его спецификация описана в RFC 5415. CAPWAP — это протокол прикладного уровня, основанный на UDP. Передает два типа сообщений на транспортном уровне. Трафик данных, который инкапсулируется и пересылается через туннель данных CAPWAP. Управляющий трафик, который управляет обменом сообщениями между точкой доступа и контроллером доступа через туннель управления CAPWAP. Пакеты данных и управления CAPWAP передаются через разные порты UDP: трафик управления (UDP 5246-порт) и трафик данных (UDP 5247-порт) [8].

При туннельной пересылке данных точки доступа инкапсулируют пакеты служебных данных, а затем передают на контроллер доступа для последующей пересылки. Пакеты данных пользователя инкапсулируются в CAPWAP- туннель, после чего контроллер пересылает их в вышестоящую сеть.

Таким образом, трафик данных и трафик управления проходит через контроллер, что упрощает реализацию политик управления безопасностью для пользователей беспроводной сети. Туннельная пересылка обычно используется вместе с сетью Off-Path. Контроллер осуществляет централизованную передачу пакетов данных, которая является более безопасной и позволяет упростить централизованное управление и контроль. Можно развернуть и настроить новые устройства с небольшими изменениями в действующей сети. Такой режим пересылки применяется для независимого развертывания WLAN или централизованного управления и контроля в крупных кампусных сетях

Исходя из проведенного исследования, была составлена модель беспроводной сети, в которой используются вышеперечисленные методы и технологии (рис. 3).

Было настроено две точки доступа (рис. 4), на которых работали три разные сети, каждая из которых работает в диапазонах 2,4 ГГц и 5 ГГЦ (рис. 5), а также включено DTLS шифрование трафика CAPWAP (рис. 6).

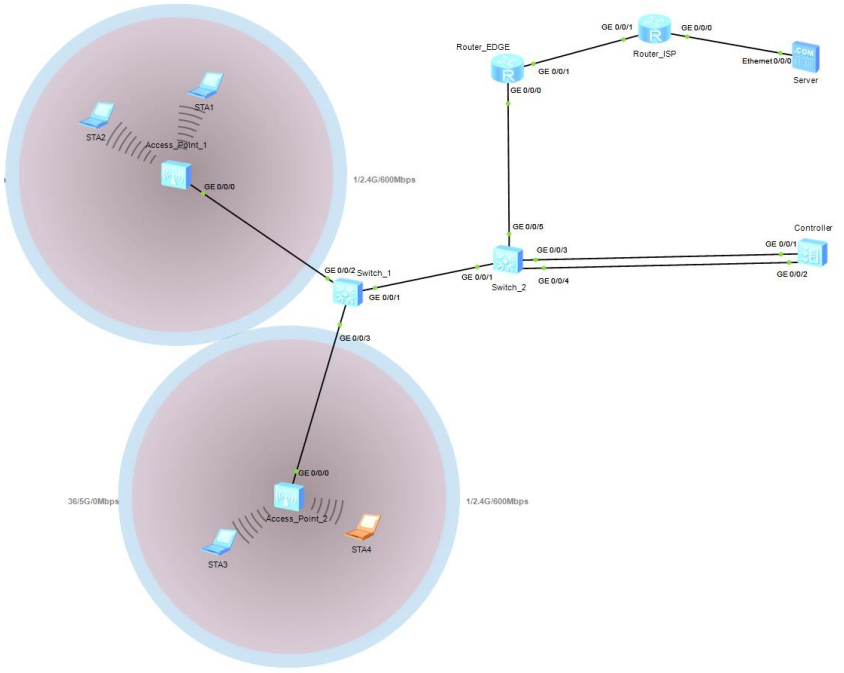

Рис. 3. Модель беспроводной сети

```
[AC]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor   : normal          [2]
--------------------------------------------------------------------------------
----------------------
ID   MAC            Name        Group       IP              Type            Stat
e STA Uptime
--------------------------------------------------------------------------------
----------------------
0    00e0-fc80-0580 accountants department1 192.168.100.252 AP7050DE        nor
  2   2M:54S
1    00e0-fcac-7320 managers    department2 192.168.100.251 AP7050DE        nor
  2   2M:50S
--------------------------------------------------------------------------------
----------------------
Total: 2
[AC]
```

Рис. 4. Результат настройки точек доступа

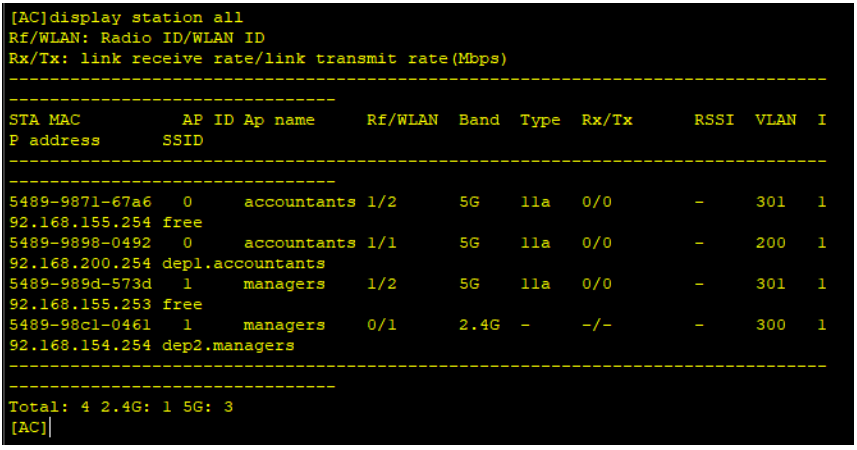

Рис. 5. Результат конфигурации сетей на точках доступа

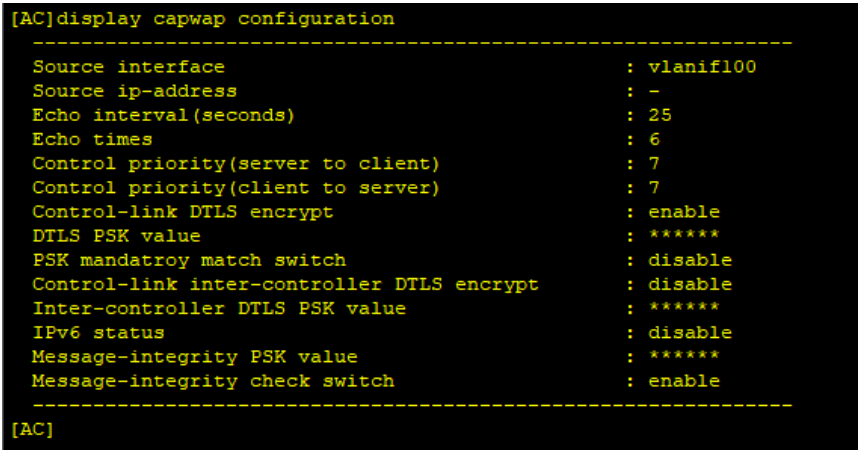

Рис. 6. Результат конфигурации DTLS шифрования

Заключение. В результате проведенной работы были изучены технические особенности функционирования контроллеров беспроводной сети, проанализированы современные методы обеспечения безопасности беспроводной сети средствами контроллера, а также смоделирована безопасная беспроводная сеть в эмуляторе Huawei

eNSP. Таким образом, нами были рассмотрены базовые функциональные возможности контроллеров беспроводной сети и перспективы их использования, а также спроектирована и апробирована топология сети с использованием таких устройств.

СПИСОК ЛИТЕРАТУРЫ

1. Новинский Д. О. Особенности беспроводных WI-FI компьютерных сетей и обеспечение их безопасности / Д. О. Новинский, Д. О. Курганов. — Текст : электронный // Российская наука и образование сегодня: проблемы и перспективы. — 2019. — № 6. — URL: https://elibrary.ru/download/elibrary_41673101_35147378.pdf (дата обращения: 02.05.2022).
2. Отакулов А. С. Безопасность беспроводной сети / А. С. Отакулов — Текст : электронный // MODERN SCIENCE. — 2020. — № 7. — URL : https://elibrary.ru/download/elibrary_43130370_33680703.pdf (дата обращения: 02.05.2022).
3. Игнатьев В. Безопасность беспроводных сетей / В. Игнатьев. — Текст : электронный // Системный администратор. — 2004. — № 1. — URL : https://www.elibrary.ru/download/elibrary_20395848_80369851.pdf (дата обращения: 02.05.2022).
4. Enterprise Network Simulator Software Installation Guide. — URL : https://support.huawei.com/enterprise/en/doc/EDOC1000006464?idPath=24030814%7C250382819%7C250382820%7C9017384 (date of the application 03.05.2022). — Text : electronic.
5. HUAWEI Networks : Партнер компании Huawei : [сайт]. — URL : https://www.huawei-networks.ru/catalog/huawei-access-controller/ac6605 (дата обращения: 06.05.2022). — Текст : электронный.
6. WLAN Architecture. — 2021. — URL: https://support.huawei.com/enterprise/ en/doc/EDOC1100156624/f342dc7/wlan-architecture (дата обращения: 07.05.2022). — Текст : электронный.
7. Построение корпоративных WLAN сетей (Best Practice). — Ч. 1. — 2021. — URL: https://forum.huawei.com/ enterprise/ru/ (дата обращения: 07.05.2022). — Текст : электронный.
8. Обзор протокола CAPWAP. — 2021. — URL: https://forum.huawei.com/enterprise/ru/%D0%BE%D0%B1%D0%B7%D0%BE%D1%80%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B0-capwap/thread/761607-100554 (дата обращения: 08.05.2022). — Текст : электронный.