СОЗДАНИЕ СЕГМЕНТА ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ АПК «БЕЗОПАСНЫЙ ГОРОД»

А.В. Крылов, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, krylov180497@yandex.ru*

УДК 004.733

Аннотация. Современные города должны соответствовать возрастающим информационным потребностям граждан и автономно обеспечивать их безопасность. Для этого сети, объединяющие аппаратно-программный комплекс (АПК) в единую структуру, совершенствуются и расширяются, появляются новые возможности и растет уровень безопасности таких сетей. Города в ближайшем будущем благодаря внедрению АПК повсеместно станут удобнее и безопаснее для каждого гражданина.

Ключевые слова: АПК «Безопасный город»; умный город; информационная безопасность; аутсайдерские атаки.

CREATING A SEGMENT OF TELECOMMUNICATIONS INFRASTRUCTURE APK «SAFE CITY»

Alexey Krylov, *Saint Petersburg state University of telecommunications named Prof. M.A. Bonch-Bruevich.*

Annotation. Modern cities must meet the growing information needs of citizens and ensure their security autonomously. To do this, the networks that unite the APK in a single structure are being improved and expanded, new opportunities are emerging and the level of security of such networks is growing. Cities, in the near future, will become more convenient and safer for every citizen thanks to the introduction of APK everywhere.

Keywords: APK «Safe city»; smart city; information security; outsider attacks.

Введение

В настоящее время очень актуальна проблема обеспечения безопасности в общественных местах. В связи с этим Правительством Российской Федерации осуществляется комплекс мер, направленных на предупреждение чрезвычайных ситуаций и повышение возможностей по ликвидации их последствий.

Характерной особенностью крупных городов, в частности Санкт-Петербурга, являются большая плотность населения, повышенная численность культурных и материальных ценностей и наличие большого количества потенциально опасных объектов. Все эти факторы определяют высокую вероятность возникновения чрезвычайных ситуаций различного характера.

По результатам анализа состояния безопасности жизнедеятельности в регионе и непосредственно в Санкт-Петербурге был сделан следующий вывод: существующие тенденции обязывают принимать решения по предотвращению вероятных катастроф и их последствий [1].

Структура АПК «Безопасный город»

Аппаратно-программный комплекс «Безопасный город» (АПК «Безопасный город») – совокупность комплексов средств автоматизации, объединенных для решения задач в сфере обеспечения защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, общественной безопасности, правопорядка и безопасности среды обитания.

Структура АПК состоит из 12 частей – автоматизированных систем, представленных на рис. 1. Перечень автоматизированных систем государственной информационной системы «Аппаратно-программный комплекс «Безопасный город» и порядок их взаимодействия описан в постановлении Правительства Санкт-Петербурга от 25.08.2016 № 759.

Рисунок 1

Все компоненты АПК «Безопасный город» объединены Единой мультисервисной телекоммуникационной сетью, которая обеспечивает функционирование системы в целом и создает единое информационное пространство для всех пользователей[1].

Целью построения и развития АПК «Безопасный город» является повышение общего уровня общественной безопасности, правопорядка и безопасности окружающей среды за счет обеспечения координации деятельности сил и служб, путем внедрения на базе муниципальных образований комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз.

Основными задачами построения и развития комплекса «Безопасный город» являются:

- формирование коммуникационной платформы для органов местного самоуправления;
- разработка единых функциональных и технических требований к аппаратно-программным средствам;
- обеспечение информационного обмена между участниками всех действующих программ;
- обеспечение информационного обмена на федеральном, региональном и муниципальном уровнях;
- создание дополнительных инструментов для оптимизации работы;
- построение и развитие систем ситуационного анализа.

[1] Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Реализация сегмента телекоммуникационной сети

Единая информационно-коммуникационная инфраструктура комплекса «Безопасный город» строится по модульному принципу с возможностью включения в единый контур управления и информационного обмена элементов уже существующей инфраструктуры муниципальных образований [2].

Для проектной реализации был выбран сегмент сети городской системы видеонаблюдения по адресу пл. Александра Невского. Данный сегмент обеспечивает: видеонаблюдение объектной площади, общественную сеть *WI-FI* для граждан, экстренную связь с полицией, интегрирование локальных сетей метрополитена и гостиницы.

На карте объекта представлено расположение телекоммуникационного оборудования и средств видеонаблюдения. Карта объекта изображена на рис. 2.

Рисунок 2

Схемы построения сети представлены на рис. 3 (физическая топология сети) и рис. 4 (логическая топология сети).

Для реализации проекта сегмента сети АПК «Безопасный город» было выбрано следующее оборудование:

- уровень ядра – маршрутизатор *Cisco ASR 9000*. Основная особенность *Cisco ASR* – физическое разделение аппаратных инструментов управления и коммутации, что позволяет значительно ускорить реализацию сетевых процессов [8];
- уровень распространения – *L3* коммутаторы *Cisco 9200*;
- уровень доступа – *L2* коммутаторы *Cisco 2960*, *IP* камеры *PST* (производитель *Shenzhen professional security technology Co.*).

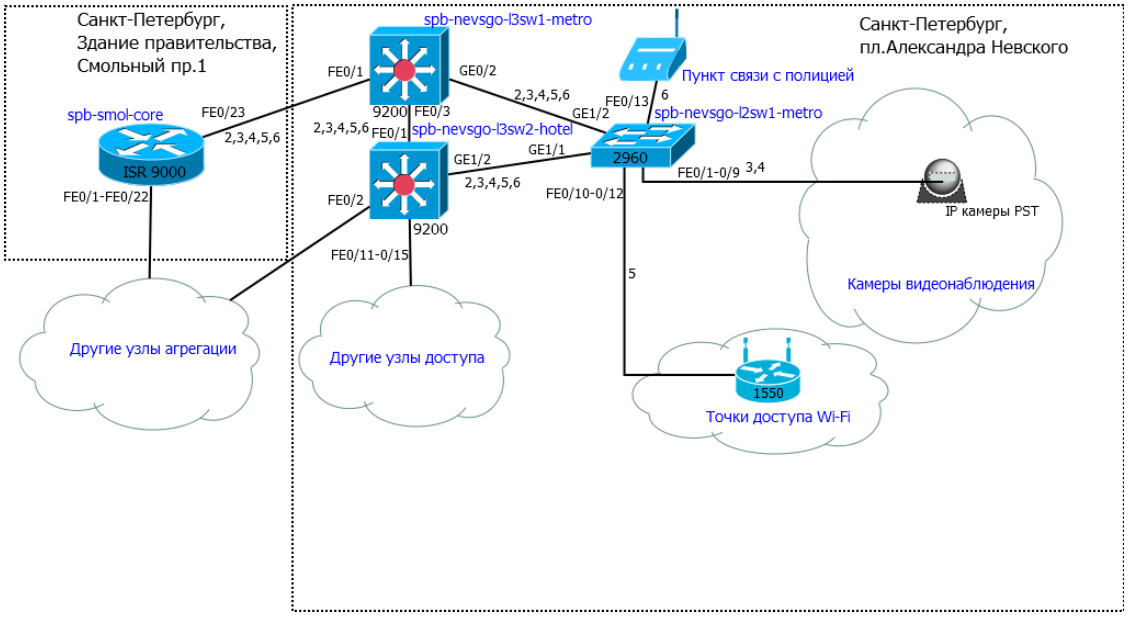

Рисунок 3

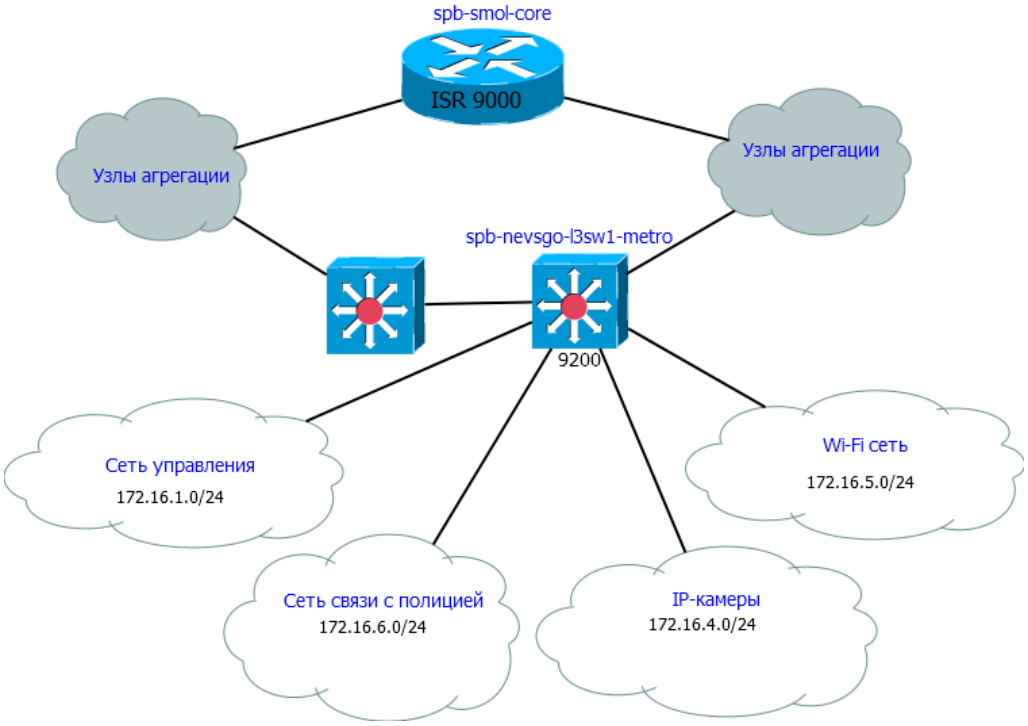

Рисунок 4

Выбранное оборудование полностью соответствует потребностям и требованиями сети АПК. Однако, есть аналоги от других производителей, например, оборудование компании *Huawei* обойдется дешевле, но у производителя *Cisco* лучшая репутация в сфере телекоммуникационного оборудования. Уровень распространения строится по кольцевой топологии, обеспечивая отказоустойчивость сети.

Основными типами угроз для сети АПК являются аутсайдерские.

Для обеспечения защищенного подключения и функционирования предложенной топологии предлагается использовать следующие протоколы и функции:

- Подключение только по протоколу *SSH*.

SSH – Secure Shell, сетевой протокол прикладного уровня, который дает возможность шифрования передаваемых данных и паролей [3];

- Использование шифрования в паролях доступа.

Каждый пароль, настраиваемый на оборудование, должен быть зашифрован;

- Разделение уровня привилегий.

Функционал операционной системы оборудования *Cisco* позволяет разделить права доступа по различным ролям (например, полный доступ или права только на просмотр настроек) [6];

- Ограничение физической доступности устройств.

Каждое устройство должно быть хорошо защищено от физического воздействия при помощи железных боксов и замков;

- Настройка сетевого времени (протокол *NTP*).

Протокол *NTP* с функцией аутентификации обеспечивает механизмы синхронизации с точностью до наносекунд, а также предлагает средства для определения характеристик и оценки ошибок локальных часов и временного сервера, который осуществляет синхронизацию. Предусмотрены возможности работы с иерархически распределенными первичными эталонами, такими как синхронизуемые радио-часы [4];

- Логирование *Syslog*.

Syslog – протокол передачи текстовых сообщений, прежде всего логов – сообщений о происходящих событиях [8]. Протокол позволяет отслеживать все действия, произошедшие в сети;

- Отключение протоколов обнаружения (*CDP, LLDP*).

CDP (англ. *Cisco Discovery Protocol*) – проприетарный протокол второго уровня, разработанный компанией *Cisco Systems*, позволяющий обнаруживать подключенное (напрямую или через устройства первого уровня) сетевое оборудование *Cisco*, его название, версию операционной системы и *IP*-адреса. Если не отключить данный протокол, злоумышленник, сумев подключиться к одному из устройств, сможет получить информацию обо всей сети [7];

- Использование протоколов *AAA*.

AAA (*Authentication Authorization and Accounting*) – система аутентификации авторизации и учета событий, встроенная в операционную систему *Cisco*, служит для предоставления пользователям безопасного удаленного доступа к сетевому оборудованию *Cisco*. Она предлагает различные методы идентификации пользователя, авторизации, а также сбора и отправки информации на сервер [5].

Как и все технологии в наше время, способы построения и функционал «Безопасного города» постоянно совершенствуются, позволяя обеспечивать безопасность городской среды автономно и повсеместно. На данный момент благодаря развитой телекоммуникационной инфраструктуре к сети АПК можно подключить любой объект – от маленького детского сада до огромных торговых центров. Функционал АПК уже сегодня очень обширен, он дает городским властям следующие возможности:

- непрерывное видеонаблюдение за каждым участком, потенциально опасным для граждан;

- интегрирование сети муниципальных образований для оперативной и защищенной связи между ними;
- обеспечение эпидемиологического контроля с помощью датчиков температуры;
- удаленное управление светофорами для уменьшения дорожной загруженности;
- распознавание лиц в толпе по видеоизображению;
- бесплатный *Wi-Fi* в общественных местах.

Однако, системам АПК «Безопасный город» еще есть куда развиваться, например, в скором будущем возможно именно с помощью сети АПК будут управляться беспилотные квадрокоптеры и общественный транспорт.

В вопросах обеспечения безопасности также есть множество возможностей по улучшению и развитию. Сеть АПК должна быть защищена безупречно и не иметь уязвимостей как от аутсайдерских угроз, так и от инсайдерских. Такой уровень защиты может быть достигнут разработкой автоматизированных средств защиты сети на основе машинного обучения.

Заключение

В статье рассмотрены вопросы проектирования и обеспечения безопасности телекоммуникационной инфраструктуры АПК «Безопасный город». Разработаны схемы организации линий связи, на которых указаны оконечные пункты, и установленное в них оборудование. В тоже время следует учитывать, что при проектировании и фактическом выполнении работ по строительству и эксплуатации сети могут быть внесены изменения, связанные с реальными проблемами на участке.

Литература

1. Официальный сайт Правительства Санкт-Петербурга [Электронный ресурс] – Режим доступа: https://kis.gov.spb.ru/proekty/bezopasnyj-gorod/ (дата обращения 11.03.2020).

2. RFC Syslog [Электронный ресурс] – Режим доступа: https://tools.ietf.org/html/rfc4716 (дата обращения 15.03.2020)

3. RFC NTP [Электронный ресурс] – Режим доступа: https://tools.ietf.org/html/rfc4716 (дата обращения 15.03.2020)

4. Wendell Odom IP *Routing in the LAN* // *Cisco Press.* 2020. – № 2. – С. 1-12.

5. Сахаров Д.В., Красов А.В., Ушаков И.А., Орлов Г.А. Защищенная модель программно-определяемой сети в среде виртуализации Kvm // Электросвязь, 2020. – № 3. – С. 26-32.

6. Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе Ipv6 // Защита информации. Инсайд, 2020. – № 1 (91). – С. 51-57.

7. Савинов Н.В., Токарева К.А., Ушаков И.А., Красов А.В., Сахаров Д.В. Исследование модели сети ЦОД на основе политик Cisco Aci // Защита информации. Инсайд, 2019. – № 4 (88). – С. 32-43.

8. Официальный сайт ООО «Cisco sistems» [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/index.html (дата обращения 09.03.2020).

9. Методические рекомендации АПК «Безопасный город» построение (развитие), внедрение и эксплуатация от 22 февраля 2015 г. № 2-4-87-12-14.