О.О. Беспрозванных, А.А. Оленников

Тюменский государственный университет, г. Тюмень

УДК 004.056.5

КОМПЛЕКС МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ДАННЫХ В СИСТЕМЕ ВИДЕОНАБЛЮДЕНИЯ ДЛЯ АДМИНИСТРАТИВНОГО ЗДАНИЯ

Аннотация. В работе представлено краткое описание проекта, а также описание мероприятий по защите данных в системе видеонаблюдения.

Ключевые слова: система видеонаблюдения, IP-видеонаблюдение, информационная безопасность, защита данных.

Информационные системы должны быть защищены как от внешних, так и от внутренних угроз, в этом может помочь система видеонаблюдения. Она поможет обеспечить контролируемую зону и вести слежение за людьми в ее пределах.

В настоящее время системы видеонаблюдения широко распространены. Инфраструктуры этих систем могут быть небольшими, в пределах одного здания или же очень масштабными, сопоставимыми размером с целым городом. Видеонаблюдение используется практически во всех сферах нашей жизни, что приводит к несомненной необходимости обеспечения информационной безопасности.

Для начала рассмотрим административное здание, для которого необходимо разработать проект системы видеонаблюдения и комплекс мероприятий по защите данных в ней. Офисное здание расположено в городе Томск и состоит из 4 этажей (первый – цокольный). Видеонаблюдение будет вестись как внутри, так и снаружи объекта, а также будет организована система видеоаналитики на входе в здание (с внутренней стороны).

Топология сети приведена на рис. 1. Она предполагает, что сервис IP-камер будет недоступен для несанкционированного доступа. Как показано на

рисунке, регистраторы, находящиеся во внутренней и внешней частях здания отнесены к разным кластерам. Используется межсетевой экран D-link NetDefend DFL-870. Также имеется два WAN порта, один из них основной, а второй резервируемый.

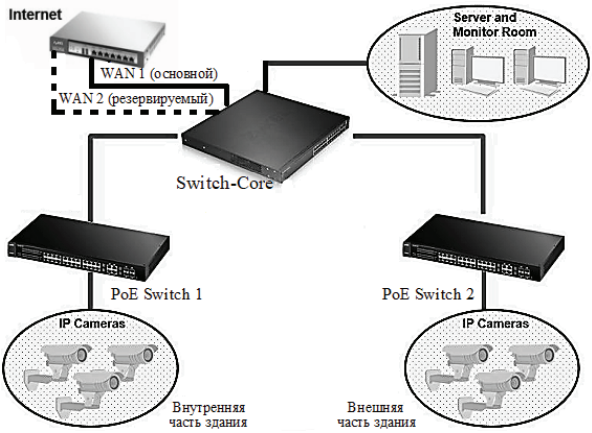

Рис. 1. Топология сети.

Вопрос кибербезопасности имеет высокое значение для систем видеонаблюдения. При получении записей с видеокамер, необходимо установить, что эти данные не были подменены или модифицированы [1].

Как известно, существует два типа видеокамер: аналоговые и цифровые. Среди цифровых, в свою очередь, выделим IP-видеокамеры, так как для проекта были выбраны именно они. IP-камера является полноценным сетевым устройством и обладает своим собственным IP-адресом [1].

Помимо очевидных достоинств, таких как более интеллектуальное видеонаблюдение, удаленный доступ к видеоархивам и возможность еще большей масштабируемости систем, с появлением IP-видеонаблюдения обозначилось множество проблем, связанных с безопасностью данных. Так, например, в 2016 году было проведено большое количество DDoS-атак, в том числе, с использованием систем видеонаблюдения, пораженных вирусами [3].

Основными угрозами безопасности видеокамер являются прослушивание и изменение трафика, а также вышеупомянутые DDoS-атаки.

Для защиты системы видеонаблюдения от несанкционированного доступа необходимо:

- *Использовать технологию VLAN для разделения трафика IP-камер.*

Технология VLAN, она же виртуальная локальная компьютерная сеть, имеет ряд преимуществ, которые позволяют выделить её как рекомендуемую для использования при построении безопасной системы видеонаблюдения.

Первым и основополагающим достоинством использования VLAN является подразделение сети на логически сгруппированные конечные устройства (рис. 2), причём отсутствует жёсткая привязка к физическому расположению компонентов. Это позволяет организовать гибкое управление и внесение изменений в трафике, проходящем по сети. Так, например, имеется возможность провести настройку коммутаторов для построения иерархии по приоритету трафика того или иного сегмента сети.

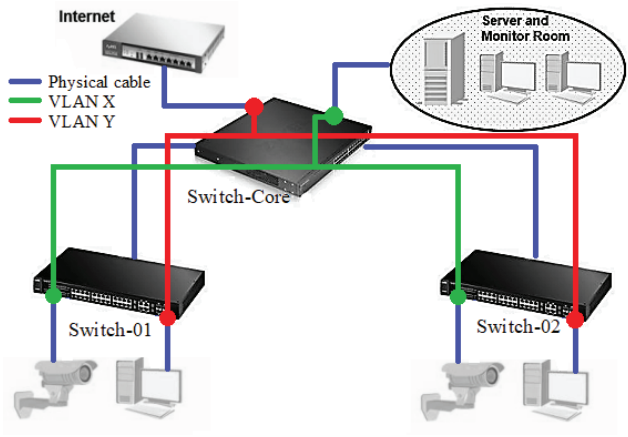

Рис.2. Схема VLAN рассматриваемой сети.

Стабильность – это второе преимущество использования VLAN. Она достигается за счет сокращения широковещательного домена, что позволяет уменьшить общую передачу всех пакетов.

Третий и наиболее важный для нас параметр – безопасность области сети, в которой работают IP-камеры. В том случае, если камеры работают в одном VLAN с иными конечными устройствами, сложится ситуация, что сеть будет открыта для IP-спуфинга.

Помимо прочего, повышается мобильность сети: облегчается добавление и перемещение устройств, а также изменение их соединений между собой.

- *Сменить пароли для входа в систему, установленные по умолчанию* [2].

Самым простым и очевидным шагом является смена данных для входа в систему, однако, очень часто этим правилом пренебрегают. Стандартная пара логин-пароль, как правило, указывается в инструкциях по эксплуатации, поэтому не стоит оставлять этот факт без внимания. Как известно, рекомендуется использовать сложную комбинацию символов, состоящую из строчных и прописных букв, цифр и знаков.

- *Внедрить фильтрацию и криптографическую защиту сетевого трафика* [4].

Подобрать оборудование, которое будет производить фильтрацию и шифрование данных перед записью в хранилище, а также стоит позаботиться о резервном копировании информации.

- *Использовать разграничение прав доступа и построение грамотной политики безопасности.*

Разграничение прав доступа позволяет не допустить превышение полномочий, например, если сотрудник имеет доступ только для просмотра видео с камер, он не сможет случайно или преднамеренно удалить запись. В случае кражи или утери пароля злоумышленник не получит полный доступа к системе.

- *Установить последние версии программного обеспечения* [2].

Не стоит забывать о поддержании прошивки камер видеонаблюдения в актуальном состоянии, так как обновления ПО направлены не только на

исправление ошибок, но и на защиту от новых вирусов и угроз, что позволяет повысить стабильность работы системы в целом.

Система видеонаблюдения интегрирована в общую локальную сеть заказчика, поэтому для достижения поставленных целей в вопросах кибербезопасности стоит учесть и внедрить совокупность всех вышеперечисленных методов, так как именно их совместное применение позволяет достичь желаемого уровня защищенности, а также предотвратить широко распространённые угрозы и риски. Помимо прочего, стоит проводить своевременный аудит для оценки текущего состояния системы с точки зрения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Алтухов А.А.Концепция защиты трафика систем видеонаблюдения / А.А. Алтухов // Вопросы защиты информации : Научная статья. – 2014. – 4 (107). – С. 15-17.
2. Взлом камер видеонаблюдения на практике [Электронный ресурс]. – URL: https://geektimes.ru/company/devline/blog/290829/ (дата обращения 08.04.2018).
3. Видеонаблюдение: 8 главных трендов на мировом рынке в 2017 году [Электронный ресурс]. – URL: http://securityrussia.com/blog/cctv-trendy2017.html#china (дата обращения: 10.04.2018).
4. Безопасность систем безопасности: защита информации IP-видеонаблюдения [Электронный ресурс]. – URL: https://infotecs.ru/about/press-centr/publikatsii/bezopasnost-sistem-bezopasnosti-zashchita-informatsii-ip-videonablyudeniya.html (дата обращения: 11.04.2018).