

Н. А. Апурин, В. А. Петров

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ И МЕТОДОВ ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ С ВОЗМОЖНОСТЬЮ ДИСТАНЦИОННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ

В настоящее время актуально построение систем комплексной защиты с возможностью дистанционного контроля и управления. Неотъемлемой частью таких систем является система обеспечения защиты информации в создаваемой комплексной системе [1].

Предлагаемые системы безопасности относятся к физической безопасности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей; показатель, отражающий статус защищенности информационной системы. Отдельные сферы деятельности, такие как системы государственного управления, банки, информационные сети и другие, требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач. ИБ достигается за счет реализации комплекса мероприятий и средств защиты, основанных на внутрифирменной **политике безопасности и анализе рисков**, допустимых для данной компании в конкретный период времени.

Определим основные виды угроз защищаемой информации, а также способы защиты.

Основные виды угроз:

— Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи;

— Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой;

— Угрозы доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации [2].

Данное исследование крайне важно, потому что оно позволяет спланировать все дальнейшие действия — реализация систем видеонаблюдения и объединение их в системе «Умный дом», а также изучить основные принципы выбора оборудования по наблюдению с помощью видеокамеры, по пожарной охране, элементам системы «Умный дом».

В первой практической части была подготовлена и внедрена модель системы безопасности с использованием аналоговой видеокамеры. Использовано следующее оборудование: видеокамера «ЕС 580», сервер с видеоплатой, роутер с выходом в Интернет.

Принцип работы данной схемы заключается в следующем: видеокамера передает видеосигнал на плату сервера. С платы сервер получает видеоданные. Полученные файлы обрабатываются для оптимизации просмотра через Интернет. Для дальнейшей трансляции и просмотра разрабатывается интернет-сайт www.artwell.ru, с которого возможно просмотреть записи системы наблюдения



за любой день, а также текущий поток с видеокамеры. Реализована возможность просмотра изображения через сотовый телефон путем уменьшения частоты кадров в секунду.

Во второй практической части было необходимо подготовить и внедрить модель системы безопасности с использованием IP-видеокамеры. Было использовано следующее оборудование: видеокамера «Trendnet WiFi VB-150», сервер, роутер с выходом в Интернет.

Принцип работы данной системы заключается в следующем: видеокамера передает поток на сервер и на роутер. Полученные сервером файлы обрабатываются для дальнейшего использования. Функция видеокамеры позволяет писать файлы с максимальным размером 50 МБ. Для реализации возможности просмотра и скачивания видео за прошедший период разработано программное обеспечение, которое собирает и ужимает все файлы в один. Благодаря этой программе 150 файлов по 50 мегабайт ужимаются примерно в 1 ГБ. Для дальнейшей трансляции и просмотра разрабатывается интернет-сайт www.5asec.ru, с которого возможно просмотреть записи системы видеонаблюдения до семидневной давности, а также текущий поток с видеокамеры. Реализована возможность просмотра изображения через сотовый телефон путем уменьшения частоты кадров в секунду [3].

В заключительной части работы проведено объединение системы видеонаблюдения и систем «Умный дом». В данной системе используются 2 видеокамеры — аналоговая камера «VB19BH-W36» и «IP DLINK DCS 5220», сервер на основе «LinuxMCE» и на платформе «Windows» с использованием «ActiveHome», датчик «CM15», датчик управления нагрузками, ламповый модуль «LW12», датчик движения «MS13», пожарная кнопка, герконы, автономный датчик дыма. Схема реализуется следующим образом: датчик движения засекает объект и передает сигнал на датчик «CM15» по радиоканалу, «CM15» передает сигнал на сервер, с которого происходит оповещение по sms, одновременно с этим сервер передает сигнал на «CM15» о подаче питания на аналоговую камеру, о начале записи с IP-видеокамеры (в нашем случае видеокамера записывает не постоянно, для экономии места на жестком диске), о включении света на ламповый модуль («CM15» передает команды по силовым линиям, используется протокол передачи данных «X10»). Также если на объект проникает нарушитель через дверь, то при открытии двери срабатывают герконы, которые подают сигнал на «CM15» [4].

Основные цели:

- разработка и внедрение системы видеонаблюдения в интернет-сайт;
- реализация системы видеонаблюдения в компании «5asec»;
- объединение реализованных систем в системе «Умный дом».

В настоящее время актуальным является построение систем комплексной защиты с возможностью дистанционного контроля и управления. Неотъемлемой частью таких систем является система обеспечения защиты информации в создаваемой комплексной системе.

Разработанная модель системы безопасности с возможностью дистанционного контроля и управления «Умный дом» позволяет обеспечить комплексную защиту для любого объекта.

СПИСОК ЛИТЕРАТУРЫ:

1. Будзинский Н. Радиосистемы охраны. Учебное пособие. М.: Владис, 2004. — 547 с. URL: <http://www.bestbook/xn-fg9/u78975>.
2. Лавриненко А. В. Периметровые средства обнаружения: современное состояние // Специальная Техника. 2001. № 5. URL: http://st.ess.ru/publications/5_2001/lavrinenko/lavrinenko.htm.
3. Михайлов В. О. Защита информации в Интернете. URL: <http://www.dss1.ru>.
4. Документация к оборудованию. URL: <http://www.vb-pto.ru>.

