значение УИД контролируемого объекта. 8. Получение в блоке логической операции XOR контролируемого объекта значения ПСП-1 блока контроля и его поступление в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока. 9. Выработка в генераторе ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока, последовательности ПСП-2. 10. Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок. 11. Декодирование в управляющем блоке полученного сигнала с помощью НКХП, идентичного НХП в контролируемом объекте. 12. Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в УС. 13. Выработка ПСП-2 управляющего блока и ее поступление в УС. 14. Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта. 15. Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма. 16. Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 17 алгоритма. 17. Вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

Список литературы

1. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена // Вестник СибГУТИ. 2018. № 1. С. 33–40.

2. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена для беспроводных систем безопасности с усложненной имитовставкой // Вестник НГУ. 2019. Т. 17, № 1. С. 18–27.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ УСТАНОВОК ДЫМОУДАЛЕНИЯ

В.Е. Галузо, В.В. Мельничук, А.И. Пинаев

При проектировании в соответствии с [1] установок дымоудаления (ДУ) в составе систем противодымной защиты (ПДЗ) в первую очередь определяется весовой, а затем объемный расход удаляемой газодымомвой смеси $L_Д$. Значение последнего определяется при нормированном [1] значении температуры удаляемых газов (более 300 °С) для подбора вентилятора. Кроме $L_Д$ для подбора вентилятора необходимо значение падения давления в сети $P_С$ установки ДУ. Давление $P_С$ рассчитывается в соответствии с [1] с учетом естественного давления газов $P_{ЕС}$, определяемого разностью удельных весов наружного воздуха и дыма (при температуре более 300 °С) и высотой шахты. При высоте шахты (здания) 50 м $P_{ЕС} \approx 300$ Па. Это давление вычитается из расчетного давления $P_С$ установки ДУ. Аэродинамические испытания установок ДУ проводятся при нормальной температуре в помещении (менее 30 °С) и параметрах Б [2] для теплого периода года для данного региона (26 °С для г. Минска). При таких температурах удельные веса удаляемого из помещения и наружного воздуха отличаются незначительно и давление $P_{ЕС}$ составляет единицы Па, и им можно пренебречь. То есть измерения объемного расхода газа, удаляемого установкой ДУ проводятся при давлении в сети отличающегося от проектного значения, а значит производительность вентилятора и объемные расходы будут отличаться, что может привести к тому, что измеренное значение объемного расхода воздуха $L_В$ будет существенно отличаться от проектного $L_Д$ (более 20 % [3]), что может быть причиной принятия решения о непригодности установки ДУ для эксплуатации.

Предлагается при проектировании установок ДУ выбор вентилятора осуществлять с учетом давления газов $P_{ЕС}$ при нормируемой температуре дыма (более 300 °С). Затем по аэродинамической характеристике выбранного вентилятора определять объемный расход удаляемого установкой воздуха при давлении в сети без учета давления $P_{ЕС}$ газов (воздуха). На основании чего определять объемный расход удаляемого через клапан ДУ воздуха $L_В$.

Список литературы

1. ТКП 45-4.02-273-2012. ПДЗ зданий и сооружений при пожаре. Системы вентиляции.
2. СНБ 4.02.01. Отопление, вентиляция и кондиционирование воздуха.
3. НПБ 23-2010. ПДЗ зданий и сооружений. Методы испытаний.

МЕТОДИКА НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СЕТИ

А.А. Горелик, Н.В. Журавский

В работе [1] для оценки защищенности узлов информационной сети предложено использовать программное средство «Сканер». В настоящей работе определен порядок настройки и эксплуатации указанного средства. Он включает в себя следующие этапы.

1. Вход в веб-интерфейс ПС «Сканер». Для этого необходимо открыть веб-обозреватель и перейти по адресу https://<IP-адрес сервера ПС «Сканер»>/. В результате будет открыто окно авторизации, в котором необходимо ввести имя пользователя и пароль.

2. В случае успешной авторизации – выбор ссылки «Задачи» в разделе «Сканирование» главного меню.

3. Запуск процесса сканирования. Для запуска стандартного сканирования следует выбрать «Мастер задач» и в открывшемся диалоговом окне указать IP-адрес или DNS-имя целевой системы (устройства). Для запуска расширенного сканирования в окне «Продвинутый мастер задач» необходимо выбрать дополнительные параметры сканирования, основными из которых являются следующие:

– «Конфигурация сканирования» – выбор предустановленной конфигурации сканирования;

– «Время запуска:» – время запуска задачи сканирования (немедленно или по расписанию);

– «Отправить отчет по электронной почте» – адрес электронной почты для отправки отчета.

4. Формирование отчета, содержащего результаты сканирования.

На основе данных, представленных в отчете, составляются рекомендации по совершенствованию механизмов защиты данных в исследованном объекте (информационной системе или информационной сети).

Список литературы

1. Горелик А.А., Бойправ О.В., Журавский Н.В. Методика анализа защищенности узлов вычислительной сети // Материалы XV Международной науч.-практ. конф. «Управление информационными ресурсами», Минск, 7 декабря 2018 г. С. 210–212.

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ ТЕХНОЛОГИИ HONEYPOT

В.И. Грицкевич, С.Н. Петров

В современном информатизированном мире для любой организации очень важно защитить свои активы от нападения злоумышленников. Чтобы приблизиться к обеспечению наиболее полной информационной безопасности, нужно быть на шаг впереди злоумышленников, таким образом, необходимо отражать атаки до наступления негативных последствий от их выполнения. Одним из таких инструментов для мониторинга поведения злоумышленников является технология Honeypot (далее – ханипот).

В ходе анализа существующих ханипотов был сделан вывод, что хорошим вариантом построения данной технологии является комбинирование автоматического подхода к решению задачи обнаружения атак и человеческих возможностей принятия решения. Архитектура такой системы может состоять из четырех различных компонентов, а именно: внешний брандмауэр, ханипот (виртуальная машина), база знаний и специальная группа SOC (Security operations center, центр реагирования на инциденты в сфере информационной безопасности) для ручного анализа журналов событий. В ней присутствуют различные модули для определения наиболее точных результатов, которые помогут администратору принимать решения на основе