си теплоносителя более «пологие», т. е. данный период является более продолжительным. В этот период эффект увеличения скорости сушки достигается за счёт того, что азот является транспортёром влаги, создавая с её парами ассоциативные группы, которые имеют большую подвижность в воздушной среде, чем отдельные молекулы воды и, соответственно, быстрее удаляются из слоя продукта, то есть молекулы азота играют роль переносчика молекул пара с поверхности древесной частицы в сушильную камеру и далее к поверхности конденсации. Кроме этого молекулы инертного газа «бомбандируют» продукт, ослабляя силы взаимодействия между молекулами в местах их попадания [8].

Из анализа результатов исследований кинетики процесса обезвоживания древесных опилок с повышенным содержанием азота в воздушной смеси теплоносителя для разной скорости установлено, что при большей скорости теплоносителя увеличивается и скорость удаления влаги из древесных опилок. Однако при этом увеличение скорости опилок имеет свой предел, обусловленный возникновением уноса опилок (особенно мелкой фракции) с теплоносителем при его скорости больше 2,5 м/с.

В процессе сушки наблюдается одновременно несколько физических процессов, происходящих в структуре древесных материалов. В то время как влажность древесины постепенно падает, температура частиц повышается и приближается к температуре осушающего агента. Поэтому, с целью исключить возгорание легковоспламеняемых мелкодисперсных составляющих смеси, температуру теплоносителя, подаваемого в сушильное оборудование, ограничивают до безопасного уровня.

Таким образом, на основании проведенных исследований среди факторов, влияющих на скорость процесса сушки, необходимо выделить следующие результаты: температуру теплоносителя, продуваемого через слой опилок; относительную скорость его движения в процессе сушки; удельную площадь поверхности частиц древесных материалов, связанную с их размером; физические свойства материалов, подвергаемых сушке.

Список литературы

1. Вулка М.Ф. Физико-химические свойства водных систем [Текст] / М.Ф. Вулка, О.Ф. Безрукова. СПб., 1991. 200 с.

2. Гинзбург А.С. Основы теории и техники сушки пищевых продуктов [Текст] / А.С. Гинзбург. М. :Пищевая промышленность, 1973. 528 с.

3. Гинзбург А.С. Технология сушки продуктов [Текст]. М.: Пищевая промышленность, 1973. 527 с.

4. Дущенко В.П. Свойства материалов как объектов сушки и методы их исследования [Текст] / В.П. Дущенко // В кн.: Интенсификация тепло-влагопереноса в процессах сушки]. Киев, Наукова думка, 1979. С. 84-93.

5. Лыков А.В. Теория сушки [Текст] / А.В. Лыков. М. : Энергия, 1968. 470 с.

6. Черноусова Н.Ю. Совершенствование процесса горячего копчения рыбной продукции с использованием импульсной ультразвуковой обработки [Текст]: автореферат дис. на степ. кан. тех. наук / Черноусова Н.Ю. Воронеж, 2009. 24 с.

7. Чудинов Б.С. Вода в древесине. [Текст] / Б.С. Чудинов. Новосибирск: Наука, 1984. 270 с.

8. Шумский К.П. Основы расчета вакуумной сублимационной аппаратуры [Текст] / К.П. Шумский, А.И. Мялкин, И.С. Максимовская. М.: Машиностроение, 1967. 223 с.

Секция «Безопасность информационных технологий», научный руководитель – Валиев М.М.

ОБЗОР ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АНАЛИЗА ПОКАЗАТЕЛЕЙ ЭНЕРГОПОТРЕБЛЕНИЯ СИСТЕМЫ

Минакова О.И.

Башкирский государственный университет, Уфа, Россия, e-mail: olgminakva@rambler.ru

Введение

В мае 2014 года компания Symantec – являющаяся пионером в создании антивирусных продуктов – публично признала обреченность антивирусных решений. Согласно Symantec, более 55% угроз невозможно обнаружить с помощью стандартного антивируса [6]. В связи с этим индустрия IT-безопасности начинает поиски новых способов обнаружения вредоносного программного обеспечения.

Целью данного исследования является изучение возможностей технологии, разработанной компанией Power Fingerprinting Cybersecurity, а также тенденций в области развития хакерских атак и развития систем защиты информации. В ходе данного исследования производился анализ и синтез материалов российских и зарубежных Интернет-источников.

Чтобы распознать компьютерный вирус антивирусным программам необходимо заранее задать критерии поиска и распознавания следов активности вредоносной программы на компьютере. Задать такие критерии для обнаружения угрозы, связанной с внедрением в работу аппаратного обеспечения, до недавнего времени было практически невозможно. В 2013 году способ обнаружения подобных угроз был представлен стартап-компанией Power Fingerprinting Cybersecurity, а критерием обнаружения были результаты анализа показателей энергопотребления системы.

Для обнаружения вредоносной программы стартап использует выявление отклонений в показателях потребления электроэнергии, вместо стандартных методов определения вирусной активности (сигнатурное сканирование, эвристический анализ и т.д.). Новый метод обнаружения направлен на выявление кибератак на автоматизированные системы управления технологическими процессами (АСУ ТП) предприятий энергетической и обрабатывающей промышленности. Представленная технология успешно обнаружила вирус Stuxnet в экспериментальной модели локальной вычислительной сети прежде, чем вредоносная программа начала свою активность [3].

Stuxnet – компьютерный червь, поражающий компьютеры на базе операционной системы Microsoft Windows. Stuxnet был обнаружен в июне 2010 года не только на компьютерах домашних пользователей, но и в системах промышленных предприятий, которые управляются автоматизированными производственными процессами.

Stuxnet стал первым компьютерным червем, который способен перехватывать и модифицировать поток данных между программируемыми логическими контроллерами марки SIMATIC S7 и рабочими станциями SCADA-системы SIMATIC WinCC фирмы Siemens. Эта программа может использоваться злоумышленниками для несанкционированного сбора данных и диверсий в АСУ ТП промышленных пред-

приятий, электростанций, аэропортов и пр. Червь использует 4 известные уязвимости системы Microsoft Windows, в том числе уязвимость «нулевого дня», которая распространяется при использовании USB-flash накопителей [4].

В эксперименте, проведенном компанией для демонстрации возможностей собственной разработки, в качестве объекта атаки был использован программируемый логический контроллер (ПЛК) Siemens S7-1200. Показатели потребления энергии снимались с помощью ближнеполевых датчиков, а осциллограмма протекающих процессов выводилась на экран коммерческого осциллоскопа. Весь процесс отслеживался с помощью рабочей станции, на которой было установлено PFP (англ. power fingerprinting – дактилоскопия электрических процессов) анализирующее ПО. Чтобы воссоздать модель АСУ ТП предприятия был использован макет, представляющий из себя резервуар для воды с установленными в нём датчиками, насосом и панелью управления оператора. ПЛК активирует насос, чтобы заполнить резервуар. Когда резервуар наполнен, котроллер отключает насос. Статус процесса отображается на панели управления оператора. Наконец PFP анализирующее программное обеспечение отслеживает показатели потребления электроэнергии, чтобы удостовериться в целостности процесса.

Для атаки было использовано ПО, использующее те же подходы, что и компьютерный червь Stuxnet. Оно модифицирует процессы обработки информации в ПЛК, но таким способом, чтобы оператор ничего не заподозрил. Цель атаки заключалась в переполнении резервуара с водой, что могло привести к потенциальной опасности разлива воды. Это позволяет наглядно представить атаку вредоносной программы на АСУ шлюзами гидроузла, которая может спровоцировать аварийный сброс воды крупного водохранилища.

Во время своей работы Stuxnet отдает команды ПЛК игнорировать показания датчиков о переполнении резервуара и продолжать набор воды, при этом червь скрывает активность насоса и показатель заполненности резервуара от панели оператора. PFP анализирующее ПО сравнивает информацию о частоте электрического тока и его мощности, потребляемыми каждым устройством с базисными показателями на этих устройствах. Базисные показатели измеряются во время выполнения системой санкционированных действий. Любые изменения в показателях потребления энергии могут свидетельствовать о сбое в программном или аппаратном обеспечении или о функционировании вредоносной программы. В случае обнаружения подобных аномалий соответствующее сообщение передается оператору АСУ ТП, который принимает решение о расследовании инцидента.

Отличительной особенностью данного метода является то, что этот метод позволяет также обнаружить скрытое присутствие Stuxnet в системе. Так как червь при невозможности навязать свои условия запуска процесса переходит в «спящее» состояние. В таком состоянии червь демонстрирует поведение, идентичное незараженной системе и вмешивается в процесс, запущенный самой АСУ ТП. Такое поведение крайне сложно распознать, используя традиционные методы обнаружения, так как при этом отсутствуют такие показатели как подозрительный сетевой трафик.

Технология также успешно проявила себя в обнаружении вредоносного ПО в системах на базе управления ОС Android, выявив отклонения показателей потребления энергии, вследствие атаки под названием «RageAgainstTheCage». Вредоносное ПО получает доступ к root-правам управления устройством, обеспечивая себе полный контроль над ним [7].

Система, разработанная Power Fingerprinting Cybersecurity, будет реализовываться в следующей комплектации:

1. Ближнеполевой датчик, позволяющий снять показания протекания электрического тока в диэлектрических и полупроводниковых структурах и получить карту распределения диэлектрической проницаемости для выявления мелких дефектов и неоднородностей [2].

2. Устройство для преобразования аналогового частотного сигнала в цифровой и вывода графика колебаний на экран монитора (осциллоскоп).

3. P2Scan – PFP анализирующее ПО, которое непрерывно анализирует сигнал и сравнивает его с базисными показателями [5].

Ближнеполевой датчик не использует разъёмы устройства для своей работы. Для снятия показаний используется антенна, представляющая из себя петлю коаксиального кабеля. P2Scan не требует установки непосредственно в систему, а функционирует на отдельной рабочей станции. Благодаря этому присутствие подобной технологии в системе невозможно обнаружить при удаленном взломе.

Стартап создан при финансировании научно-исследовательского подразделения американской армии DARPA, а также при участии министерства внутренней безопасности США. По идее авторов, эту технологию планируется внедрить в автоматизированных системах управления, а именно, в программируемых логических контроллерах и других устройствах [1]. Это позволит избежать необходимости приобретать программное и аппаратное обеспечение дополнительно для внедрения данной технологии в систему защиты информации предприятия.

Таким образом, результатом данного исследования является сформировавшееся понятие о концепции технологии обнаружения вредоносных программ на основе анализа показателей потребления электроэнергии, а также о развитии угроз компьютерной безопасности и средств противодействия им.

Заключение

Хакерские атаки на объекты критической инфраструктуры государственного значения могут иметь катастрофические последствия для национальной безопасности. Существующие технологии обеспечения информационной безопасности предприятия основываются на методах устранения известных или выявленных непосредственно в ходе атаки уязвимостей, обеспечении информационной безопасности периферии АСУ (межсетевые экраны, контроль доступа, физическая изоляция компьютеров), анализе сетевого трафика и поиске вирусных сигнатур. Однако с развитием информационных технологий разрабатываются новые способы несанкционированного воздействия на информационные системы, способные обходить названные методы обеспечения информационной безопасности. Именно поэтому открытие PFP технологии является новой ступенью в истории развития систем информационной безопасности.

Список литературы

1. Вычисление уязвимостей по потреблению энергии [Электронный ресурс]. – Режим доступа:https://xakep.ru/2015/02/05/power-fingerprinting (дата обращения: 12.02.2015).

2. Фадеев А.В. Ближнеполевая СВЧ микроскопия и её использование для определения характеристик элементов твердотельной СВЧ электроники [Электронный ресурс]. – Режим доступа:http://www.sgu.ru/sites/default/files/dissertation/2014/10/22/dissertaciya_fadeeva.pdf (дата обращения: 14.02.2015).

3. New Technology Detects Cyberattacks By Their Power Consumption [Электронный ресурс]. – Режим доступа:http://www.darkreading.com/analytics/security-monitoring/new-technology-detects-cyberattacks-by-their-power-consumption-/d/d-id/1318669 (дата обращения: 12.02.2015).

4.Stuxnet [Электронный ресурс]. – Режим доступа:http://www.securitylab.ru/news/tags/Stuxnet (дата обращения: 13.02.2015).
5. Startup finds malware intrusions by keeping an eye on processor radio frequencies [Электронный ресурс]. – Режим доступа:http://www.networkworld.com/article/2875517/security0/startup-finds-malware-intrusions-by-keeping-an-eye-on-processor-radio-frequencies.html (дата обращения: 14.02.2015).
6. Symantec: антивирусная индустрия обречена [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/452523.php (дата обращения: 13.02.2015).
7. Tiny Changes in Energy Use Could Mean Your Computer Is Under Attack [Электронный ресурс]. – Режим доступа:http://www.technologyreview.com/news/507966/tiny-changes-in-energy-use-could-mean-your-computer-is-under-attack/ (дата обращения: 14.02.2015).

Секция «Информационные технологии в науке, технике и образовании», научный руководитель – Преображенский А.П.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МЕНЕДЖМЕНТЕ

Болюх Е.В.

Воронежский институт высоких технологий
Воронеж, Россия, e-mail: app@vivt.ru

Рассмотрим основные средства, позволяющие достичь эффективное функционирование менеджеров в компании, обеспечивающих поддержку процессов управления.

На настоящий момент получила распространение электронная почта, которая позволяет достичь отправки, транспортировки, отслеживания и получения менеджерами корреспонденции; ее работа поддерживается со стороны сетевых информационных систем разного уровня и ранга. Активно применяются в информационных системах и возможности графического представления (когда требуется сделать отображение процессов, объектов, закономерностей и т. п. в виде столбцовых, секторных диаграмм, гистограмм, а также разных видов схем, карт и др.).

Помимо графики используют программные средства, дающие возможности создания демонстрационного материала; их используют в виде иллюстраций при подготовке совещаний, докладов и выступлений. Основными преимуществами презентаций могут быть названы совместное отображение информации в виде числа, текста, таблицы, образа, мультимедийных составляющих и графиков; их можно демонстрировать на широкоформатных демонстрационных жидкокристаллических экранах.

С целью того, чтобы эффективно организовать рабочее время менеджерами могут быть освоены такие программы, которые обеспечивают соответствующее планирование работ с разбивкой на различные интервалы времени, проведение корректировки планов, учета и анализа их выполнения и др. Говорят о так называемых «электронных секретарях».

В качестве базы в них можно выделить функцию, связанную с планированием рабочего дня, а также проведением контроля и анализа выполнения плана. Процессы планирования строятся на базе того, что распределяется ресурс по рабочему времени среди разными работами в течение определенных интервалов времени (месяц, неделя, день); при этом необходимо правильным образом сделать оценку реальной трудоемкости по каждой из работ.

Когда выполняются такие работы часто появляются потребности в том, чтобы корректировались сроки их начала, окончания и очередности. Указанные изменения связаны с разными факторами, которые не всегда можно учесть зарание (вследствие болезней, срочных дополнительных работ, указаний со стороны вышестоящего руководства и др.). Такие функции в информационной системе могут быть реализованы на базе «деловых дневников», «записных книжек», «рабочих блокнотов», «личных картотек» и т. д.

Список литературы

1. Землянухина Н.С. О применении информационных технологий в менеджменте / Успехи современного естествознания. 2012. № 6. С. 106-107.
2. Родионова К.Ю. Глобализация мировой экономики: сущность и противоречия / Вестник Воронежского института высоких технологий. 2012. № 9. С. 185-186.
3. Гуськова Л.Б. О построении автоматизированного рабочего места менеджера / Успехи современного естествознания. 2012. № 6. С. 106.

ОСОБЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В ТУРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Гащенко И.А.

Воронежский институт высоких технологий
Воронеж, Россия, e-mail: app@vivt.ru

Сформировавшийся в последнее время рынок, связанный с туристическими услугами нуждается в том, чтобы была надежная и достоверная информация о том, каково состояние рынка, а также развивались клиентские сервисы, которые основываются на разных возможностях, которые обеспечиваются за счет современных средств коммуникаций. То есть, должно быть соответствующее информационное обеспечение. Именно на основе информационных потоков можно создать совокупность связей среди производителей туристических услуг.

В них отмечают не только потоки данных, но и платежи.

Туризм, относящийся как к международным и внутренним компетенциям, представляют собой области с растущим применением современных информационных технологий. Идет интегральное развитие систем информационных технологий, которые используются в туризме, на основе рассмотрения систем резервирования, создания телеконференций, бронирования, и др.

Каждая из частей указанных систем оказывает заметное влияние на то, каким образом идет развитие других частей. В системах, связанных с управлением туристическими объектами в качестве базовой основы могут использоваться компьютерные глобальные сети.

Исходя из анализа результатов, полученных на основе информационных технологий, появляются возможности для того, чтобы дать рекомендации того, каким образом проводить оценку состояния туристических областей и в какие из направлений наиболее эффективным способом можно осуществлять вклад средств.

По мере того, как идут процессы развития индустрии туризма, происходит уменьшение уровня безработицы в регионах, заметным образом идет увеличение потоков денежных средств в местные бюджеты.

Для регионального уровня решение проблемы формирования требуемого информационного обеспечения может быть осуществлено на базе гибридизации туристических, географических и экономических информационных систем.

Используют электронные карты, для того, чтобы применять результаты исследований, связанных с геологической, почвенной, ботанической, а также зоо-