и нажимаем *ОК*. После проделанных действий нужно будет пройти шесть пунктов, в которых: выбираются поля, которые будут выводиться на экран, будет автоматически установлена связь по ключам в таблице, выбирается порядок сортировки и вид формы. В завершение выбираем *Save form and modify it in the Form Designer*, вводим название, выбираем куда сохранить, нажимаем *Finish.*

На данном этапе созданы формы: справочник констант, справочник соотношения вредных производственных факторов должности и подразделению, справочник для добавления техпроцессов, оборудования.

Завершающим этапом, является создание отчётов. Для создания отчёта, нужно открыть окно *Project Manager*, где можно выбрать вкладку *All* и в разделе *Documents – Report* нажимаем на кнопку *New,* после нажатия на кнопку *New*, в появившемся окне выбираем *Report Wizard*.

На этом этапе созданы отчёты: перечень производственных факторов на рабочих местах в ОАО «Коминтерн», список профессий (должностей) подлежащих медосмотру, список работников ОАО «Коминтерн», подлежащих периодическому медицинскому осмотру на n-год и комплексная гигиеническая оценка условий труда работающих.

А.И. Кучеров (УО «ГГУ им. Ф. Скорины», Гомель)
Науч. рук. **В.Д. Левчук**, канд. техн. наук, доцент

ПУТИ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ УЗЛОВ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

В процессе функционирования вычислительной системы возникают сбои и отказы как аппаратуры, так и программных средств входящих в состав этой вычислительной системы. Для своевременного реагирования на сбои и отказы возникающие в процессе функционирования вычислительной системы, необходимо доподлинно знать состав аппаратных и программных средств этой системы. При запуске вычислительной системы происходит ее самодиагностика или другими словами POST-диагностика (Power-On Self Test). POST – Программа, расположенная в микросхеме BIOS, загружается первой после включения компьютера. BIOS (Basic Input/Output System – базовая система ввода-вывода). Программа системного уровня, предназначенная для первоначального запуска вычислительной системы, настройки оборудования и обеспечения функций ввода/вывода. BIOS записывается

в микросхему постоянной памяти, которая расположена на системной плате.

Программа POST-диагностики определяет и проверяет установленное оборудование, настраивает устройства и готовит их к работе. При самотестировании, возможно, будет обнаружена неисправность оборудования, тогда процедура POST будет остановлена с выводом соответствующего сообщения или звукового сигнала. Если же все проверки прошли успешно, самотестирование завершается вызовом встроенной подпрограммы для загрузки операционной системы. Ну а если же программой будет выявлена серьезная ошибка, работа системы будет остановлена с выдачей звуковых сигналов, которые укажут на возникшую неисправность. У разных производителей системных плат от ведущих производителей BIOS, такие как: AMI BIOS, Award BIOS, Phoenix BIOS, существуют свои системы подачи сигналов, где набор коротких и длинных сигналов будет соответствовать определенной критической ошибке.

Но звуковое сопровождение не всегда присуще какой-либо критической ошибке и поэтому при процедуре самотестирования POST появление критической ошибки будет указываться сообщением диагностики.

POST-диагностика, является первым этапом обеспечения надежности функционирования узлов локальной вычислительной сети. Для более существенного повышения надежности эксплуатации вычислительной системы применяют и другие методы обеспечения надежности. Одним из наиболее эффективных методов обеспечения надежной работы вычислительной системы, является дублирование или резервирование ее узлов. В идеале все узлы вычислительной системы должны иметь двойника, который будет немедленно вступать в работу при выходе из строя основного узла. Если у каждого узла вычислительной системы будет не один, а два, три, четыре, и более дублирующих узлов. То надежность вычислительной системы возрастет в несколько раз, но ее цена возрастет многократно. А эти затраты не всегда оправданы. Для обеспечения безотказной работы вычислительной системы, очень часто достаточно проводить профилактические работы по ее обслуживанию.

Помимо надежности аппаратных средств надежность функционирования вычислительной техники напрямую связана с надежностью использования программных средств и привилегиями (правами) пользователей.

Пользователь может выполнять большое количество действий. Но не все из них пользователь имеет право и должен выполнять.

А информация может быть как общего, личного, так и служебного использования.

Для повышения надежности вычислительной системы администратор должен иметь возможность управлять правами пользователей локальной вычислительной сети и следить за выполнением их служебных обязанностей. Обеспечить эти возможности предназначено, как встроенное в операционную систему, так и другое системное программное обеспечение.

Каждый пользователь или группа пользователей в операционной системе обладают определенными правами. Действия, которые пользователь может выполнять в операционной системе, строго определены и описаны. В общем случае возможностей у пользователя много. Пользователь может выполнять большое количество различных операций, на которые он может иметь или не иметь прав. Эти операции связаны как с работой на локальном компьютере, так и при работе в локальной вычислительной сети.

Чем выше привилегии пользователя, тем выше у него права и соответственно возможности. Всеми правами в операционной системе обладают только администраторы системы. Для управления правами пользователей в операционной системе в настройках имеется возможность администрирования, где можно назначить права пользователя.

Пользователь может выполнять большое количество действий. Но не все из них пользователь имеет право и должен выполнять. А информация может быть как общего, личного, так и служебного использования.

Для повышения дисциплины руководство организаций и предприятий должно иметь возможность управлять правами пользователей локальной вычислительной сети и следить за выполнением их служебных обязанностей.

Современные операционные системы от версии к версии совершенствуют системы, отвечающие за безопасность. Войти в операционную систему возможно только зарегистрированному пользователю. Он должен знать зарегистрированное имя пользователя и его пароль. Если компьютер подключен к компьютерной сети с доменами в качестве рабочей станции, то операционная система потребует помимо имени и пароля, еще и имя домена. Только при совпадении этих трех составляющих пользователю будет разрешен вход в систему. То есть пользователь пройдет аутентификацию.

Обеспечить эти возможности предназначено как встроенное в операционную систему, так и другое системное программное обеспечение.

На рисунке 1 показана упрощенная схема защиты вычислительной техники от несанкционированного использования.

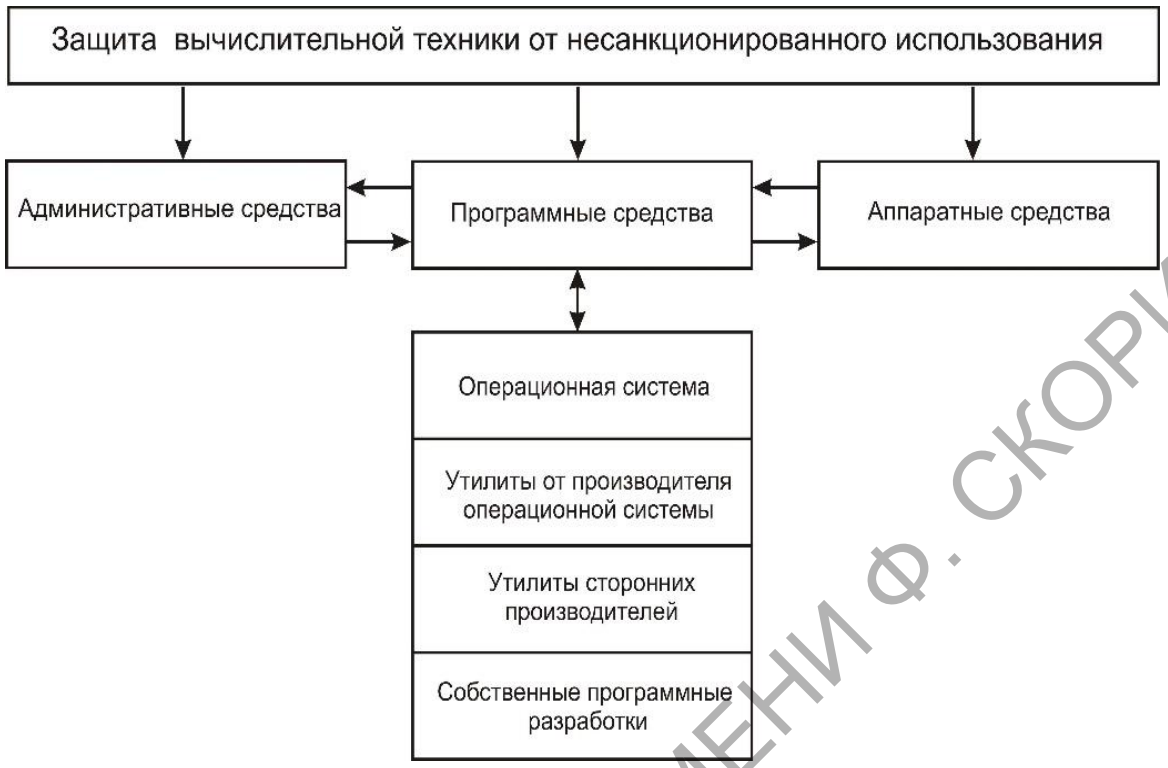

Рисунок 1 – Защита вычислительной техники
от несанкционированного использования

Исходя из рисунка 1 видно, что надежность вычислительной системы так же зависит, от защиты вычислительной техники от несанкционированного использования, которая слагается из трех составляющих: административные средства, программные средства, аппаратные средства.

П.Ю. Лаврук (УО «ГГУ им. Ф. Скорины», Гомель)
Науч. рук. **В.Н. Кулинченко,** ст. преподаватель

ПРОБЛЕМА ПЕРЕПОЛНЕНИЯ ТАБЛИЦЫ MAC-АДРЕСОВ В ШИРОКОВЕЩАТЕЛЬНОМ ДОМЕНЕ СЕТИ УО «ГГУ ИМ. Ф. СКОРИНЫ»

В настоящее время широко распространена технология BYOD (Bring Your Own Device), которая позволяет учащимся/работникам приносить свои устройства (ноутбуки, планшеты, смартфоны и т. д.) на место учебы / работы.