6) Наличие сетевого режима, где используется несколько компьютеров, объединенных для эмуляции взаимодействия средств связи.

На данный момент существующие программы для подготовки войск связи можно разделить на 3 группы:

Автономный (включающий 3 вида):

1) (индивидуальный) обеспечивает отработку навыков и повышение специальных знаний на самостоятельной подготовке;

2) обеспечивает отработку действий обучаемых при выполнении практических занятий, тренировок, групповых учений и групповых занятий в составе одной учебной группы;

3) обеспечивает решение задач, связанных с проведением тактико-специального учения кафедры связи, в составе нескольких учебных групп.

Групповой обеспечивает обучение слушателей при взаимодействии с другими специализированными тренажерами.

Комплексный обеспечивает решение задач, связанных с проведением оперативно-командного штабного учения.

Использование компьютерных средств обучения позволяет разгрузить преподавателя, увеличить заинтересованность студентов и курсантов в предмете, дает возможность решения задач на стыке предметов разных циклов, более наглядной подачи материала за счет анимации, графических вставок, динамических рисунков, видеоклипов, слайд-шоу, звукового сопровождения, что позволяет быстрее осваивать и лучше запоминать учебный материал. Благодаря усилению эмоциональной составляющей увеличивается темп урока на 10-15%.

Список использованных источников:

1. Балыкина Е.Н. Компьютерные технологии обучения: истоки и развитие информатизации образования – 1999. - №1. – С. 49-66.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К АВТОМАТИЗИРОВАННОМУ РАБОЧЕМУ МЕСТУ

Пипкин Е.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Утин Л.Л.

В современном мире информация играет ключевую роль в решении различных вопросов, поэтому остро стоит вопрос о надежной защите информации различного характера при помощи технических средств и различного программного обеспечения.

Предотвращение утечек представляет собой технологии предотвращения утечек конфиденциальной информации из информационной системы, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. Необходимость их использования стала упоминаться в стандартах и нормативных документах. Специализированные технические средства для защиты от внутренних угроз стали массово выпускаться только после 2000 года.

Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хеш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д.

Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, стеганографии и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления.

Таким образом можно подвести итог и сказать, что основной задачей DLP-систем, что очевидно, является предотвращение передачи конфиденциальной информации за пределы информационной системы.

Список использованных источников:
1. Александр Панасенко, Илья Шабанов. Сравнение систем защиты от утечек (DLP) - часть 1, 2011

ВОЕННЫЕ КОМПЬЮТЕРНЫЕ БАЗЫ ДАННЫХ КАК СРЕДСТВО ПОДДЕРЖАНИЯ ВЫСОКОЙ БОЕВОЙ ГОТОВНОСТИ ТЕХНИКИ СВЯЗИ ПОДРАЗДЕЛЕНИЙ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Стружинский В.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сасновский А.А.

Современные средства связи играют ключевую роль в системе управления войсками как в тактическом, так и оперативном звене управления. От их работоспособности зависит обмен информацией всех видов в системе управления войсками (силами) и оружием. При неполадках средств связи необходим комплекс мероприятий по немедленному ремонту и возвращения в строй средств связи, для их дальнейшего боевого применения.

Работа на реальных образцах требует определенных материальных и больших временных затрат, а также наличия соответствующих условий для работы на определенных средствах связи.

База данных (БД) – это организованная структура, предназначенная для хранения, изменения и обработки взаимосвязанной информации, преимущественно больших объемов.

Основные преимущества баз данных перед традиционными средствами хранения информации:

1) Компактность – информация хранится в БД, нет необходимости хранить многотомные бумажные картотеки;

2) Скорость – скорость обработки информации (поиск, внесение изменений) компьютером намного выше ручной обработки;

3) Низкие трудозатраты – нет необходимости в утомительной ручной работе над данными;

4) Повышенная безопасность – заключается в защите данных от незаконного несанкционированного доступа.

Информацией, хранящейся в БД, может быть всё что угодно: каталог продукции, информация о клиентах, контент веб-сайта или методы починки средств связи. Для обеспечения доступа к информации, хранящейся в базе данных, а также для управления ею, применяют систему управления базами данных (СУБД). СУБД — это комплекс