ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

УХТИНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра ИСТ

Курсовой проект

Дисциплина: «Проект управления базами данных»

Тема:

«Обеспечение защиты данных в системе «Составление расписания»

Выполнил

студент группы ИСТ-2-04

Петров М.В.

Проверила

доцент кафедры ИСТ, к. т. н.

Николаева Н.А.

Ухта 2008

**Содержание:**

**Введение**

1. **Информационные ресурсы и пользователи системы**
2. **Среда функционирования системы**
3. **Классы защищенности функциональной системы**
4. **Горизонтальная оболочка сети**
5. **Механизм защиты вертикальной структуры сети**
6. **Организационные мероприятия, направленные на повышение**

**уровня информационной безопасности в учреждении**

**Вывод**

**Список литературы**

**Введение**

В данной курсовой проекте рассматривается вопрос обеспечения защиты данных в системе «Составление расписания», разрабатываемой для Воркутинского медицинского училища, занимающегося обучением студентов медицинским специальностям в г.Воркута. Система создается для автоматизации процесса составления расписания, контроля и учета работы преподавателей, расчета нагрузки преподавателей на следующий учебный год, формирования отчетов о прочитанных часах.

Предлагаемая система должна позволять: уменьшить затраты времени на учет отработанных часов преподавателей за истекший период, экономить рабочее время сотрудника и облегчить его работу в оперативности получения и обработки информации связанной с учебным процессом, хранить данные в более удобном компактном виде, что существенно повысит скорость доступа к информационным ресурсам, а также обеспечит надёжную защиту от потери информации и несанкционированного доступа к ней.

В работе рассматривается вопрос обеспечения защиты данных в системе, разрабатываемой для учебной части и методы практической реализации обеспечения безопасности этих данных.

Целью проекта разработка политики информационной безопасности для системы «Составление расписания».

Разработчиком системы является студент группы ИСТ-03, Хромцовой А.И., Заказчиком системы является ГОУ СПО «Воркутинское медицинское училище» в лице директора Кречетниковой Ирины Петровны.

**1.** **Информационные ресурсы и пользователи системы**

В разрабатываемой системе в зависимости от используемых ролей настраиваются права конкретного пользователя, при этом оговаривается набор доступных ему информационных ресурсов и перечень операций, которые он может выполнять в каждой из них (Таблица 1).

В данной системе используются ресурсы :

Список преподавателей – это список преподавателей, которые на данный момент могут вести определенные дисциплины.

Расписание звонков – расписание пар во время которых могут проводится учебные дисциплины на данном предприятии.

Список групп – перечень групп которые обучаются по нашему расписанию

Расписание занятий – Расписание занятий в состав которого входят: название предметов, время начала и окончание занятий, фамилии преподавателей и дисциплины которые они ведут, номер аудитории в котором проводятся занятия.

Расписание за истекший период – архив расписания за истекший период.

Список аудиторий – список всех аудиторий в учебном заведении.

Таблица 1 «Матрица доступа»

|  |  |  |  |
| --- | --- | --- | --- |
| Объекты | Пользователи | | |
| Секретарь уч.час. | Зав.уч.части | Администратор |
| Список преподавателей | ПР | ПРДУ | Н |
| Расписание звонков | ПРДУ | ПРДУ | Н |
| Список групп | ПР | ПРДУ | Н |
| Расписание занятий | П | ПРДУ | Н |
| Расписание за истекший период | П | П | Н |
| Список аудиторий | ПРДУ | ПРДУ | Н |
| Права и группы | Н | Н | ПРДУ |
| Регистрационный журнал | Н | Н | ПРДУ |

Условные обозначения:

П – просмотр данных;

Р – редактирование;

Д – добавление данных;

У – удаление данных;

Н – нет доступа.

К выделенным ресурсам в системе «Составление расписание» имеют доступ следующие группы лиц:

Заведующая учебной части: имеет право на просмотр редактирование и удаление и добавление данных, составления отчета за истекший период, просмотр расписания за истекший период.

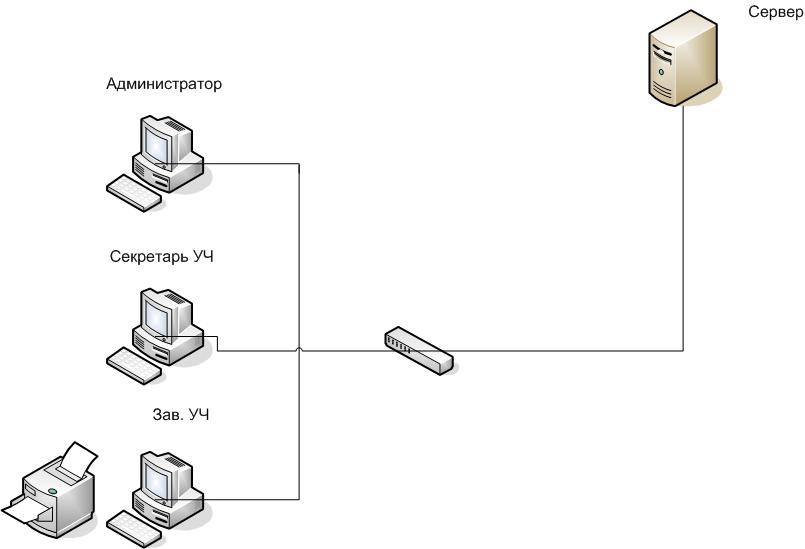
Секретарь учебной части: имеет право на просмотр всех данных, на редактирование списка преподавателей, на редактирование и на удаления и добавления данных к объекту расписания звонков, запрет на права и группы и на регистрационный журнал.

Администратор: не имеет права на просмотр данных, а имеет права на задание группы пользователей и наделение их соответствующими правами.

**2. Среда функционирования системы.**

Все пользователи системы, а также сервера баз данных соединены в компьютерную сеть. Компьютеры пользователей соединены между собой устройством (Switch – 8 портовым), которое позволяет объединить компьютеры в небольшую локальную сеть. Общая пропуская способность сети составляет 10/100 Мбит/с и позволяет осуществлять полноценную загрузку сервера системы и использовать современное программное обеспечение. Это осуществляется с помощью сетевых кабелей неэкранированная витая пара(UTP — Unshielded twisted pair) пятой категории.

**Витая пара (англ. twisted pair)** — вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), для уменьшения взаимных наводок при передаче сигнала, и покрытых пластиковой оболочкой.



**3. Класс защищённости разрабатываемой подсистемы**

Все классы оценки автоматизируемых систем разделяют на 3 группы, которые различаются особенностями обработки информации:

**3 группа:** классифицирует АС, в которой работает один пользователь, допущенный ко всему объёму информации АС, относящейся к одному уровню конфиденциальности (3А, 3Б).

**2 группа:** классифицирует АС, в которой пользователи имеют одинаковые права ко всей информации и вся она размещена на одном уровне конфиденциальности (2А, 2Б).

**1 группа:** классифицирует многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности, и не все пользователи имеют права доступа ко всей информации (1А, 1Б, 1В, 1Г, 1Д).

Разрабатываемая система относится к первой группе, т. к. она является многопользовательской. В системе предусматривается разграничение прав доступа пользователей к данным (каждый пользователь имеет доступ только к тем данным, которые необходимы только ему). В то же время информация, с которой работает система, не имеет ни один из грифов секретности, а носит чисто конфиденциальный характер (например место работы преподавателя-совместителя и его должность). Таким образом, классом защиты нашей системы будет являться 1Г. (См. таблицу 1)

Таблица 1 «Требования по защите, предъявляемые к 1Г.».

|  |  |  |
| --- | --- | --- |
| № п/п | Подсистемы и требования | 1Г |
| 1 | 2 | 3 |
| *1.* | *Подсистема управления доступом* |  |
| 1.1. | Идентификация, проверка подлинности и контроль доступа субъектов: |  |
|  | в систему; | + |
|  | к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; | + |
|  | к программам (процессам); | + |
|  | к томам, каталогам, файлам, записям, полям записей. | + |
| *2.* | *Подсистема регистрации и учета (аудит)* |  |
| 2.1. | Регистрация и учет: |  |
|  | входа/выхода субъектов доступа в/из системы (узла сети); | + |
|  | выдачи печатных (графических) выходных документов; | + |
|  | запуска/завершения программ и процессов (заданий, задач); | + |
|  | доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; | + |
|  | доступа программ, субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, програм­мам, томам, каталогам, файлам, записям, полям записей; | + |
| 2.2. | Учет носителей информации. | + |
| 2.3. | Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ н внешних накопителей. | + |
| *3* | *Подсистема обеспечения целостности* |  |
| 3.1. | Обеспечение целостности программных средств и обрабатываемой информации. | + |
| 3.2. | Физическая охрана средств вычислительной техники и носителей информации. | + |
| 3.3. | Периодическое тестирование СЗИ НСД. | + |
| 3.4. | Наличие средств восстановления СЗИ-НСД. | + |

**4. Горизонтальная модель сети**

Данная сеть нуждается в защите информации, передаваемой по сети. Информация может быть подвергнута изменению, удалению, хищению, что приведет учреждение к потерям. Для разграничения доступа к информации на сервере будет установлена СУБД MS SQL 2005 и организован доступ к серверу со всех клиентов. Следовательно, получение, заполнение и редактирование информации будет происходить средствами сервера СУБД, что позволяет разграничивать доступ к информации средствами самой СУБД. АС будет доступна только секретарю учебной части и заведующей учебной части.

Вся информация будет храниться на сервере с установленной системой управления базами данных (СУБД) и будет организован доступ к серверу со всех клиентов посредством локальной сети учреждения.

**4.1 Описание возможных угроз**

В общем случае угрозы безопасности сети учреждения можно разделить на две большие группы: внутренние и внешние.

**Внешние угрозы:**

1. Несанкционированный доступ к каналам передачи данных. Данная угроза может возникнуть в тех случаях, когда посторонний человек сможет подключиться к сети передачи данных, причем подключение может происходить любым образом.

**Внутренние угрозы:**

1. Несанкционированный доступ к основным ресурсам: серверы, активное оборудование
2. Несанкционированный доступ к персональному компьютеру пользователя
3. Несанкционированный доступ к принтерам, работающим с конфиденциальной информацией
4. Подмена рабочего места пользователя. Эта угроза возникает в результате замены компьютера пользователя другим и подмены IP-адреса. В этом случае, данные, предназначенные для пользователя, попадают в посторонние руки.

**4.2 Меры по устранению угроз безопасности сети**

Для ликвидации угроз необходимо разработать организационные мероприятия*:*

* ***Для обеспечения защиты активного оборудования от несанкционированного доступа*** к нему (угроза № 2), необходимо его разместить под охрану. Обеспечить доступ к нему и выдачу ключей лицам, обладающим такими полномочиями, например руководителю отдела.
* ***Для защиты*** ***от несанкционированного доступа к компьютеру пользователей*** (угроза № 3) необходимо использовать пароли. **Пароль** — это последовательность букв, цифр и других символов, с помощью, которой система проверяет, действительно ли это тот самый пользователь, который имеет данную учетную запись и право доступа к ресурсам.

К паролям предъявляются определённые требования:

* + - пароль не должен содержать данных, которые как-то связаны с пользователем (дата рождения, адрес и др.);
    - пароль должен сочетать в себе как символы, так и числа;
    - пароль должен содержать от 8-10 символов;
    - Для усложнения доступа к компьютеру и его ресурсам, необходимо предусмотреть пароли BIOS. Также нужно физически заблокировать доступные и не используемые порты.
    - Необходима периодическая смена паролей
* ***Несанкционированный доступ к принтерам, работающим с конфиденциальной информацией*** (Угроза № 4). Сетевые принтеры, работающие с конфиденциальной информацией (какой преподаватель сколько часов отвел), должны стоять отдельно. Возможно решение общего использования принтеров при непосредственном присутствии около принтера: документ, посланный на печать, возможно, распечатать только при идентификации и аутентификации пользователя, пославшего документ, на самом принтере.
* ***Для того чтобы избежать* *подмены рабочего места пользователя*** (угроза № 5), помещение во внерабочее время должно находиться под замком. Ключ должен выдаваться на основании распоряжения директора лицам, оговоренным в нём.

Во избежание подмены оборудования пользователя необходимо сделать привязку MAC-адреса сетевого интерфейса к коммутатору, т.е. разрешить доступ к данному порту определённому сетевому устройству. Существует также ряд неявных угроз, которые могут возникнуть в процессе функционирования активного оборудования, например сбой в электропитании, выход из строя винчестеров, пожар.

Для предотвращения последствий от сбоя рекомендуется использовать:

1. Фильтры питания;
2. Источники бесперебойного питания;
3. Автономные генераторы.
4. Средства пожаротушения.

**4.3. Поддержка работоспособности системы.**

Для поддержки работоспособности системы необходимо наладить:

1. поддержку пользователей системы, а именно необходимо расписать все возможные случаи поведения системы и действия пользователей в этих ситуациях.
2. поддержку программного обеспечения, а именно иметь в наличии все необходимые инсталляционные пакеты используемых программ.
3. поддержку аппаратного обеспечения, а именно резерв активного оборудования (в т.ч. коммуникационных кабелей), наличие источников бесперебойной работы.
4. регламент конфигурационного управления, а именно регламент подключения новых пользователей (перемещение/увольнение) - ОРМ регламент на копирование и архивирование данных/файлов - ОРМ
5. регламент восстановления работоспособности системы при экстренных ситуациях/авариях – ОРМ
6. для обеспечения точности контрольных журналов, которые могут потребоваться при расследовании или в качестве свидетельства при наложении дисциплинарных взысканий, необходимо правильно установить системные часы компьютеров. Неточные контрольные журналы могут помешать таким расследованиям и подорвать доверие к такому свидетельству;
7. должен быть утвержден регламент антивирусной защиты: определены настройки мониторов для рабочих мест пользователей и администратора, периодичность обновления антивирусных баз.

**5. Механизмы защиты вертикальной структуры сети**

Для повышения надёжности защиты информации в сети необходимо защищать её на каждом уровне модели OSI.

Физический уровень:

Данный уровень отвечает за кодирование передаваемых сигналов в среде передачи данных. На этом уровне происходит преобразование поступающих со всех остальных уровней битов (0 и 1) в электрические сигналы. В соответствии с этим, для избежания воздействия различных электромагнитных наводок, которые могут привести к искажению передаваемой информации, необходимо использовать для передачи данных специальные экранированный кабель.

Канальный уровень:

Так как на данном уровне семиуровневой модели OSI происходит работа с MAC-адресами сетевых интерфейсов (адресами сетевых карт), то с целью устранения такой угрозы, как подмена рабочего места пользователя, необходимо произвести привязку MAC-адресов к конкретным портам активного оборудования, например, коммутатора.

Привязка MAC-адресов будет выглядеть примерно следующим образом:

[разрешить доступ MAC-1 к порту Port-1]

После выполнения такой операции к порту 1 коммутатора будут иметь доступ только компьютеры с адресами сетевых интерфейсов MAC-1. Устройства с другими сетевыми картами уже не смогут получить доступ к портам данного коммутатора.

Сетевой уровень:

Сетевой уровень отвечает за маршрутизацию, т.е. за выбор оптимального пути и доставку пакета данных адресату. Так как наша сеть состоит только из 3 рабочих станций и 1 сервера, которые между собой соединены коммутатором то вся маршрутизация настраивается на отдельных рабочих станциях.

Транспортный уровень:

На данном уровне необходимо организовать списки доступа (ACCESS – листы). Например:

[Разрешить сервису Service-1 адреса IP-1 доступ к сервису Service-1 адреса IP-2]

[Разрешить сервису Service-2 адреса IP-1 доступ к сервису Service-2 адреса IP-2]

[Разрешить сервису Service-5 адреса IP-3 доступ к сервису Service-5 адреса IP-2]

[Остальное запретить]

Такие списки доступа можно настроить на каждом компьютере.

Прикладной уровень:

Это уровень сетевой модели, отвечающий за взаимодействие пользовательского приложения и сетью. На данном уровне необходимо осуществлять идентификацию (проверку наличия данного пользователя в списке) и аутентификацию (проверку достоверности имени и пароля) пользователей. При этом необходимо следить за тем, чтобы пользователи периодически осуществляли смену пароля, причём новый пароль должен значительно отличаться. Беспарольных пользователей в системе быть не должно.

Также на данном уровне необходимо произвести разделение прав доступа пользователей к информации на сервере.

Защита ОС:

На всех пользователях данной системы желательно установить операционную систему Windows XP Professional. На сервере баз данных для большей защищённости находящейся на нём информации должна быть установлена ОС Windows 2003 Server.

При инсталляции и настройке ОС рекомендуется:

1. Необходимо поставить все существующие для ОС сервиспаки;
2. Опускать ненужные сервисы, при этом необходимо периодически проверять включенные сервисы с целью выявления изменений, которые могут произойти, например, при установке нового ПО или АО (На сервере с конфиденциальной информацией не должно быть таких сервисов, как telnet, ftp, http);
3. По возможности не использовать удалённое администрирование;
4. Постоянно контролировать процессы, запущенные в системе. Администратору необходимо знать каждый процесс и для чего он запускается;
5. Поставить на компьютеры последнюю версию хорошего антивируса (AVP, DrWEB, ...) и регулярно обновлять антивирусные базы. Также необходимо политикой безопасности запретить всем пользователям, кроме администратора, отключать антивирус. Обязательно наличие механизмов регистрации процессов, их анализа и распознавания угроз системе;
6. Выполнять проверку целостности, путем вычисления значения хэш-функции (некий аналог контрольной суммы) от заранее определенного набора критичных файлов системы и сравнения этого значения с эталоном. Проверка может проводиться как программными, так и аппаратными средствами;
7. Все пользователи должны иметь пароли, устойчивые к прямому перебору, т.е. содержать буквенные, цифровые и специальные символы в разных регистрах и иметь длину не менее 10 символов. Таким образом, пароль типа Nb6$iL78@+&67K будет подбираться прямым перебором несколько лет, пароль не должен нести смысловую нагрузку, как, например: quake, doom, password и т.д.;
8. Учитывать социальный фактор: не записывать пароль на бумажках, не сообщать пароль кому-либо, игнорировать письма от якобы системного администратора сообщить логин и пароль и т.д.;
9. Пользователи, не имеющие прав администратора, не должны иметь доступ к системным файлам, реестру и т.д. Например, файл MSV\_0.dll, отвечающий за проверку подлинности пароля при локальном входе в систему, может быть скопирован и изменен таким образом, что любой пароль для любого пользователя будет считаться верным.

Прикладное и общесистемное ПО:

1. На сервере и клиенте запрещено иметь средства разработки;
2. Категорически запрещено вести разработку и эксплуатацию ПО на промышленных ресурсах. Для этих целей должны быть выделены отдельные ресурсы;
3. Каждый субъект должен иметь доступ только к тем объектам, который ему разрешён в соответствии с матрицей доступа.

Защита СУБД

В качестве сервера необходимо использовать MS SQL Server 2005. Необходимо выполнения следующих мероприятий по защите сервера СУБД.

Защита СУБД не ограничивается только внутренними защитными механизмами самой СУБД. Необходимо также защитить и операционную систему, под управлением которой работает СУБД.

К примеру, MS SQL Server не обеспечивает возможность блокировки учетной записи пользователя базы данных в случае серии неудачных попыток аутентификации. Это позволяет злоумышленнику осуществлять различные атаки на систему идентификации/аутентификации, например, пытаться подобрать имена пользователей, зарегистрированных в СУБД, и их пароли. Второй пример уязвимости - невозможность переименования учетной записи системного администратора базы данных (sa), что также позволяет осуществлять злоумышленнику попытки подбора пароля администратора СУБД.

Существует ряд уязвимостей в СУБД, которые могут привести не только к компрометации информации в базах данных, но и компрометации всей сети в целом. Эти уязвимости появляются вследствие расширения стандартных возможностей SQL-серверов. Например, использование расширенной хранимой процедуры (extended stored procedure) xp\_cmdshell позволяет выполнять функции операционной системы из командной строки так, как будто удаленный пользователь СУБД работает за консолью сервера баз данных. При этом функции, вызываемые при помощи процедуры xp\_cmdshell, выполняются с привилегиями той учетной записи, под управлением которой загружен SQL-Server.

Программы типа "троянский конь" могут быть легко созданы путем модификации системных хранимых процедур. Например, несанкционированный доступ к паролю пользователя может быть получен при его смене с помощью всего одной строчки кода. При изменении пароля, который обычно хранится в зашифрованном виде в таблице master.dbo.syslogins, указанный "троянский конь" позволит увидеть пароль пользователя в открытом виде, сохраненный в таблице spt\_values. Поэтому:

* Доступ к данным осуществляется только через системы ролей, которые назначаются системным администратором и утверждаются руководством предприятия;
* Выполняется резервное копирование базы данных.
* Установка источника бесперебойного питания, для повышения надежности электропитания на сервере.

**6. Организационные мероприятия, направленные на повышение уровня информационной безопасности в учреждении**

Проведение организационных мероприятий является не только наиболее эффективным, но и дешевым средством защиты информации.

Для защиты автоматизируемой системы было бы неплохо утвердить следующие организационные мероприятия:

* Необходимо осуществлять охрану помещений, в которых находится активное оборудование, а также организация учета ключей.
* Должен быть разработан регламент на использование паролей.
* Должен быть разработан регламент на проведение инвентаризации.
* Должны быть распоряжение на выдачу конфиденциальной информации в документальном виде.
* Должен быть разработан регламент о резервном копировании, который описывается тем, кто отвечает за эти действия, а также график их выполнения.
* Должен быть выдан запрет на использование переносных устройств информации (Flash – память, диски).
* Разграничение доступа к сетевым ресурсам
* Должен быть разработан регламент на копирование и хранение архивов.
* Должно быть произведено утверждение политики безопасности.
* Должен быть разработан регламент о получении сведений при перемещении по службе (увольнении): на основании приказов об увольнении служащих или их переводе в другие подразделения необходимо удалить учётную запись, либо изменить права доступа соответственно.
* Должен быть разработан регламент на использование антивирусного ПО.
* Регламент на профилактику: установка patch-ей: при обнаружении уязвимого места в программном обеспечении установить соответствующий patch.
* Регламент на проведение восстановительных работ и порядок действий.

**Вывод**

В данном курсовом проекте были рассмотрены методы и средства, которые необходимо применить для защиты информации, циркулирующей в системе «Составление расписания», от возможных угроз.

По перечисленным методам и средствам можно отметить, что разрабатываемая система «Составление расписания» по классификации защищённости автоматизированных систем относиться к классу 1Г.

Таблица:3 «Требования по защите, предъявляемые к 1Г. В нашей системе».

|  |  |  |
| --- | --- | --- |
| № п/п | Подсистемы и требования | 1Г |
| 1 | 2 | 3 |
| *1.* | *Подсистема управления доступом* |  |
| 1.1. | Идентификация, проверка подлинности и контроль доступа субъектов: |  |
|  | в систему; | + |
|  | к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; | + |
|  | к программам (процессам); | + |
|  | к томам, каталогам, файлам, записям, полям записей. | + |
| *2.* | *Подсистема регистрации и учета (аудит)* |  |
| 2.1. | Регистрация и учет: |  |
|  | входа/выхода субъектов доступа в/из системы (узла сети); | + |
|  | выдачи печатных (графических) выходных документов; | + |
|  | запуска/завершения программ и процессов (заданий, задач); | + |
|  | доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; | + |
|  | доступа программ, субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, програм­мам, томам, каталогам, файлам, записям, полям записей; | + |
| 2.2. | Учет носителей информации. | + |
| 2.3. | Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ н внешних накопителей. | +\- |
| *3* | *Подсистема обеспечения целостности* |  |
| 3.1. | Обеспечение целостности программных средств и обрабатываемой информации. | + |
| 3.2. | Физическая охрана средств вычислительной техники и носителей информации. | + |
| 3.3. | Периодическое тестирование СЗИ НСД. | + |
| 3.4. | Наличие средств восстановления СЗИ-НСД. | + |

Таким образом, можно отметить, что разрабатываемая система соответствует классу безопасности 1Г (см. Таблица 1), кроме пункта 2.3, так как освобождение оперативной памяти возможно только на рабочих станциях с помощью перезагрузки компьютера, на сервере же необходимо установить специальное ПО (например, анализатор механизма очистки оперативной памяти НКВД 2.5, который выполняет инструментальную проверку работы механизмов системы защиты информации АС, выполняющих очистку (обнуление, обезличивание) данных в освобождаемых областях оперативной памяти ЭВМ, выводит на экран (визуализирует) содержимое проверяемой области оперативной памяти и формирует отчет о проведенной проверке и ее результате, выводит его на экран и в файл по указанию оператора), но это предполагает значительные материальные вложения для предприятия, разработка же самим предприятием данного ПО невозможна, так как это очень громоздкий проект и требует больших вложений трудовых и денежных ресурсов.

**Список литературы**

1. Основы компьютерных сетей.: Б.Д. Виснадул. – М.: Издательский дом "Вильямс", 2002. – 656с.
2. Информационная безопасность компьютерных систем и сетей: В.М. Шаньгин. – М.: Издательский дом "Форум", 2008. – 416с.
3. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.:ил.