ЗАЩИТА И СОХРАННОСТЬ ИНФОРМАЦИИ БАЗ ДАННЫХ

Обеспечение безопасности данных на предприятии представляет собой целый комплекс поэтапных мер по их защите.

Законодательство Российской Федерации в области защиты информации

Вопросы правового обеспечения защиты информации занимают все более значительное место в законодательстве Российской Федерации. В приведенном далее списке указаны *основные нормативные правовые акты в области информационной безопасности:*

Конституция Российской Федерации.

Закон РФ от 05.03.1992 № 2446-1 «О безопасности».

Закон РФ от 23.09.1992 № 3521-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

Закон РФ от 23.09.1992 № 3526-1 «О правовой охране топологий интегральных микросхем».

Закон РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах».

Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».

Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Государственные стандарты и руководящие документы:

• по защите от НСД к информации:

ГОСТ Р 50922-96. Защита информации. Основные термины и определения

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования

ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

•по криптографической защите и ЭЦП:

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р 34.10-94 (2001). Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

ГОСТ Р 34.11-94. Функция хеширования

•по защите от утечки по техническим каналам:

ГОСТ Р В50170-92. Противодействие иностранной технической разведке. Термины и определения ГОСТ 29339-92. Защита информации от утечки за счет ПЭМИН. Общие технические требования

ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.

Требования безопасности к серверам баз данных

Корпоративные данные большинства предприятий, организаций, как правило, хранятся в базах данных, управляемых серверами баз данных. Современные серверы баз данных должны удовлетворять следующим требованиям:

- ***масштабируемость*** – отсутствие существенного снижения скорости выполнения пользовательских запросов при пропорциональном росте количества запросов и аппаратных ресурсов, используемых сервером баз данных;
- ***доступность*** – возможность всегда выполнить запрос;

- ***надежность*** – минимальная вероятность сбоев, наличие средств восстановления данных после сбоев, инструментов резервного копирования и дублирования данных;
- ***управляемость*** – простота администрирования, наличие средств автоматического конфигурирования;
- ***наличие средств защиты данных от потери и несанкционированного доступа***;
- ***поддержка доступа к данным с помощью Web-служб***;
- ***поддержка стандартных механизмов доступа к данным*** (таких как ODBC, JDBC, OLE DB, ADO.NET).

Несоответствие сервера баз данных какому-либо из этих требований приводит к тому, что даже у неплохого по другим потребительским свойствам сервера баз данных область его применения оказывается весьма ограниченной. Так, сервер баз данных с плохой масштабируемостью, успешно применявшийся при небольшом объеме обрабатываемых данных, оказывается непригодным в случае увеличения их количества. Именно поэтому лидеры рынка серверов баз данных стремятся производить продукты, удовлетворяющие всем вышеперечисленным требованиям.

Современные компьютеры - серверы представляют собой мощные персональные компьютеры, имеющие до 4- х процессоров, оперативную память до 64 Ггбайт, несколько жестких дисков с общим объемом памяти 3,6 Тбайт. Наиболее известными производителями компьютеров - серверов являются фирмы Hewlett Packard, Dell, FUJITSU-SIEMENS, IBM, ACER.

Как правило, между клиентским приложением и базой данных, хранящейся на сервере, не существует прямой связи. Между ними дополнительно встраиваются особые программные модули, позволяющие клиентскому приложению получать доступ к базе данных. Такие модули называются ***механизмами доступа к данным***.

Существует два основные способа доступа к данным из клиентских приложений:

- использование прикладного программного интерфейса;
- использование универсального программного интерфейса.

Английское название программных интерфейсов - Application Programming Interface (API).

Прикладной программный интерфейс представляет собой набор функций, вызываемых из клиентского приложения. Такие функции инициируют передачу запросов серверу баз данных и получение от сервера результатов выполнения запросов или кодов ошибок, которые затем обрабатываются клиентским приложением. Прикладной API обеспечивает быстрый доступ к данным, но может работать только с СУБД данного производителя, а замена ее повлечет за собой переписывание значительной части кода клиентского приложения. Такие API не подчиняются никаким стандартам и различны для разных СУБД.

Универсальный программный интерфейс обычно реализован в виде библиотек и дополнительных модулей, называемых *драйверами*. Библиотеки содержат некий стандартный набор функций или классов, нередко подчиняющийся той или иной спецификации, т.е. стандартизованы. Пользователь имеет возможность настроить универсальный API под необходимый формат базы данных, не изменяя при этом программный код клиентского приложения.

Достоинством прикладных программных интерфейсов является их высокое быстродействие, а недостатком – необходимость изменения программного кода приложения при изменении формата базы данных.

Достоинством универсальных программных интерфейсов является возможность применения одного и того же API для доступа к разным форматам баз данных, при том, однако, снижается быстродействие обработки данных из-за наличия дополнительного программного драйвера.

Наиболее популярными среди универсальных механизмов доступа к данным являются Microsoft Data Access Components (MDAC) и Borland Database Engine (BDE). Основными компонетнтами MDAC являются Open Database Connectivity (ODBC), OLE DB и ActiveX Data Objects (ADO).

Классы защиты автоматизированных систем (АС)

Нормативной базой является документ *«Автоматизированные системы. Защита от несанкционированного доступа к информации (НСД). Классификация автоматизированных систем и требования по защите информации»*. Дифференция подхода к определению средств и методов защиты основывается на обрабатываемой информации, составу АС, структуре АС, качественному и количественному составу пользователей и обслуживающего персонала. Главными **этапами классификации АС** являются:

- создания и анализ исходных данных;
- поиск основных признаков АС, нужных для классификации;
- анализ выявленных признаков;
- присвоение АС определенного класса защиты;

К *основным параметрам определения класса защищенности* АС относятся:

- уровень конфиденциальности информации в АС
- уровень полномочий субъектов доступа АС к конфиденциальной информации
- режим обработки информации в АС (коллективный или индивидуальный)

Выделяют **девять классов** защищенности АС от НСД к информации. Каждый класс имеет минимальный набор требования по защите. Классы можно кластеризовать на 3 группы. Каждая группа имеет свою иерархию классов.

- ***Третья группа*** — определяет работу одного пользователя допущенного ко всем данным АС, размещенной на носителях одного уровня конфиденциальности. Группа имеет два класса — 3Б и 3А
- ***Вторая группа*** — определяет работу пользователей, которые имеют одинаковые права доступа ко всем данным АС, хранимой и (или) обрабатываемой на носителях разного уровня конфиденциальности. Группа имеет два класса — 2Б и 2А
- ***Первая группа*** — определяет многопользовательские АС, где одновременно хранится и (или) обрабатываются данные разных уровней конфиденциальности, и не все пользователи имеют доступ к ней. Группа имеет пять классов - 1Д, 1Г, 1В, 1Б, 1А

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- криптографической;
- регистрации и учета;
- обеспечения целостности.

В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования в соответствии с таблицей 1.

Обозначения к таблице:
« - »: нет требования к текущему классу
« + »: есть требования к текущему классу

Таблица 1 — Требования к АС

Подсистемы и требования	Группа 3		Группа 2		Группа 1				
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
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	—	—	—	+	—	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	—	—	—	+	—	+	+	+	+
Управление потоками информации			—	+	—	—	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа (выхода) субъектов доступа в (из) систему(ы) (узел 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	—	—	—	+	—	+	+	+	+
изменения полномочий субъектов доступа	—	—	—	—	—	—	+	+	+
создаваемых защищаемых объектов доступа	—	—	—	+	—	—	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	—	+	—	+	—	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	—	—	—	—	—	—	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной	—	—	—	+	—	—	—	+	+

Подсистемы и требования	Группа 3		Группа 2		Группа 1				
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
информации									
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	—	—	—	—	—	—	—	—	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	—	—	—	+	—	—	—	+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	—	—	—	+	—	—	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	—	+	—	+	—	—	+	+	+

ЗАДАНИЕ:

Изучить требования к автоматизированным системам, определить и обосновать необходимый класс защищенности АС от НСД к информации для:

1. АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной;

2. АС техникума, хранящей информацию о студентах: персональные данные, сроки обучения, специальность, результаты обучения и т.д.