**Лекции №13: Особенности процесса разработки**

**Цель:** ознакомить студентов с ключевыми этапами процесса разработки программного обеспечения, выделить особенности, связанные с обеспечением безопасности на всех стадиях разработки, и объяснить важность применения принципов безопасного программирования для предотвращения уязвимостей и угроз.

Следует разработать процедуры для усиления защиты и улучшения выполненных настроек. Необходимо также выполнить один из шагов, соответствующий вашему случаю.

* Убедитесь, что создана резервная копия содержимого и настроек сервера, имеются средства и ресурсы для восстановления системы в случае неполадок.
* Настройте защищенный периметр сети для отделения интернета от интранет-сети. Важную роль в периметровой защите играют маршрутизаторы, сетевые экраны и "демилитаризованные зоны" (*DMZ*).
* Используйте дополнительные параметры защиты каталога IIS и фильтрацию сетевых пакетов Windows 2000 во внутренней сети, в которой нет брандмауэра, блокирующего и/или ограничивающего доступ на IP-адреса и домены, находящиеся вне сети.

При удаленном управлении сайтом (т.е. он расположен на сервере *интернет*-провайдера или компании веб-хостинга) он должен быть настроен на безопасное удаленное управление.

В данной лекции обсуждаются меры по обеспечению безопасности управления и функционирования сети. Вы научитесь создавать резервные копии и восстанавливать систему при нарушении безопасности и в непредвиденных ситуациях. Также вы узнаете о фильтрации пакетов, периметровой защите и настройке *IIS* для работы в различных сетевых архитектурах. Наконец, научитесь безопасно осуществлять удаленное управление.

### План восстановления

В политику безопасности нужно включить процедуры по восстановлению сайта. Основой этой стратегии являются регулярно обновляемые резервные копии, а также резервирование данных при каждом обновлении сайта, даже если не подошло время запланированного обновления.

Каждый раз при внесении изменений в конфигурацию сайта следует создавать набор дисков экстренного запуска и восстановления. Диски экстренного восстановления (*ERD*) возвращают веб-*сайт* в рабочее состояние после сбоев, вызванных вторжением вируса или вредоносной атакой, выведшей из строя операционную систему. Всегда создавайте резервную копию реестра при создании этих дисков, так как *информация* о настройках *Windows* 2000 и *IIS* хранится именно в реестре. После проведения трудоемкой работы по обеспечению безопасности сайта было бы глупо не сохранить восстанавливаемый набор настроек.

Как же создаются резервные копии содержимого сайта? На общедоступных сайтах используется автоматическое резервирование, например, зеркала дисков или дуплексирование. Использование зеркал дисков заключается в подключении второго диска к контроллеру диска сервера для одновременной записи данных на оба диска. Дуплексирование данных заключается в установке второго контроллера, чтобы у каждого диска был собственный *контроллер*. Такие системы позволяют создавать полную копию диска сервера, которую можно сразу подключить к работе при выходе из строя основного диска. Но и эти системы не гарантируют полной безопасности и не устраняют необходимость создания копий на съемных носителях вручную, так как и они уязвимы к различным атакам. Например, *файловый вирус* может легко распространиться на оба диска.

Резервные копии на съемных носителях позволяют физически отделить их от работающей системы, расположить копии в защищенном месте на случай чрезвычайных обстоятельств, таких как пожар, ограбление или стихийное бедствие. Храните резервные копии в удаленном месте, иначе вы решите только половину проблемы.

#### Экстренное восстановление

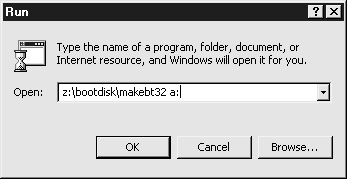
В общем случае при повреждении системы используется диск установки Windows 2000. Однако на случай более основательных сбоев нужно создать набор гибких дисков для запуска компьютера и выполнения восстановления, если программа установки системы не распознает на поврежденном диске образ предыдущей системы. Набор гибких дисков состоит из загрузочных установочных дисков и диска экстренного восстановления.

##### Создание загрузочных дисков установки

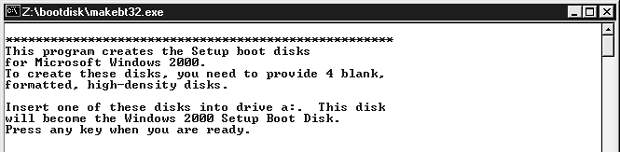
Для подготовки гибких дисков используется установочный компакт-диск Windows 2000. Вам понадобятся четыре пустых отформатированных 3,5-дюймовых дискеты объемом 1,44 Мб для установочных дискет и одна дискета для диска экстренного восстановления системы. Пометьте первые четыре дискеты меткой "Установочный диск Windows 2000" с номерами от одного до четырех, а пятую дискету пометьте как "Диск экстренного восстановления Windows 2000".

Для создания установочных дискет Windows 2000 выполните следующее.

1. Вставьте компакт-диск установки Windows 2000 в компьютер и выберите команду Start\Run (Пуск\Выполнить). Появится диалоговое окно Run, показанное на рисунке ниже.



1. Введите команду Z:\bootdisk\makebt32 a: и нажмите на OK ( Z: – это обозначение устройства для чтения компакт-дисков, a: – привод гибких дисков).
2. При выполнении команды окно консоли (см. ниже) выдаст инструкцию, согласно которой нужно вставить первый диск. Следуйте инструкциям программы и меняйте диски до тех пор, пока все установочные дискеты не будут готовы.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/6/files/06_02.gif)

Теперь у вас имеется набор загрузочных установочных дискет на случай, если система не загрузится с жесткого диска или с компакт-диска. Эти дискеты позволят восстановить Windows 2000, о чем мы расскажем далее.

##### Подготовка диска экстренного восстановления

Следующим шагом является создание диска экстренного восстановления Windows 2000 (*ERD*). При возникновении системной ошибки или повреждении сервера этот диск используется для восстановления главных системных файлов с компакт-диска исходной установки Windows 2000 без полной переустановки системы.

При помощи *ERD* можно выполнить следующие действия по восстановлению.

* *Проверка и восстановление загрузочного сектора*. Проверяется связь *загрузочного сектора* системного *раздела диска* с файлом загрузки операционной системы NTLDR и его повреждение (или изменение).
* *Проверка и восстановление среды загрузки*. Если необходимые для загрузки файлы отсутствуют или повреждены, то они переписываются с установочного компакт-диска Windows 2000.
* *Проверка системных файлов Windows 2000 и замена отсутствующих или поврежденных файлов*. На загрузочном системном диске Windows 2000 сравниваются системные файлы с файлами установочного компакт-диска, проверяется наличие всех файлов и отсутствие повреждений. Любой файл, не прошедший данный тест, заменяется.

**Совет**. При начальной установке Windows 2000 и IIS в загрузочном системном разделе создается папка с именем %systemroot%\*Repair*, в которую записывается информация о настройках системы. Не следует изменять или удалять данную папку. Исключением из правила является процесс укрепления системы (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)), а именно, удаление файла Security *Accounts Manager* (Диспетчер безопасности учетных записей). Эта мера сводит к минимуму угрозу атак, направленных на файлы с паролями. Но данное действие делает невозможным восстановление паролей и учетных записей пользователей при восстановлении системы. Восстановить учетные записи и пароли можно с помощью восстановления файла SAM, сохраненного во время последнего полного резервирования системы.

##### Содержимое диска экстренного восстановления

В программе резервного копирования Windows 2000 есть мастер для создания диска экстренного восстановления *ERD*. *ERD* создается посредством копирования отдельных файлов из папки Windows 2000 %systemroot%\*Repair* на гибкий диск (см. [табл. 6.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3527?page=2" \l "table.6.1)).

*ERD* не восстанавливает пользовательские данные или программы. Он просто хранит список файлов, установленных в системе, в файле Setup.log. Это текстовый файл, в котором записаны сведения о компонентах Windows 2000 и их расположении, установленных на сервере. Содержимое файла Setup.log можно просмотреть в любом текстовом редакторе. На [рисунке 6.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3527?page=3" \l "image.6.1) показан пример файла Setup.log.

|  |  |
| --- | --- |
| Таблица 6.1. Файлы, хранящиеся на *ERD* | |
| **Имя файла** | **Описание** |
| Autoexec.nt | Используется для инициализации среды MS-DOS. |
| Config.nt | Используется для инициализации среды MS-DOS. |
| Setup.log | Журнал, хранящий записи об установленных файлах и их расположении, а также CRC (контрольную сумму файла), которая используется в процессе экстренного восстановления. Файл имеет атрибуты "только чтение", "системный" и "скрытый" и является невидимым, если My Computer (Мой компьютер) не настроен на отображение всех файлов. |

Каждая строка журнала содержит подробную информацию о файлах и каталогах системной папки сервера (папка в *загрузочном разделе*, содержащая исполняемые файлы, шрифты драйверов и другие файлы). В конце строки записывается CRC (контрольная сумма файла) в двоичном виде. Она вычисляется программой резервирования/восстановления и показывает размер файла. При использовании диска экстренного восстановления *ERD* с помощью CRC определяется, был ли текущий системный файл изменен (удален, поврежден и т.д.). В этом случае программа восстановления заменит исходный файл новым.

Диск *ERD* не содержит копии файлов реестра. Тем не менее, при создании диска можно зарезервировать файлы из каталога %systemroot%\*Repair*.

**Вопросов для закрепления материала:**

1. Что такое план восстановления, и почему он важен для обеспечения безопасности веб-сайта?
2. Какие шаги необходимо выполнить при создании резервных копий содержимого и настроек сервера?
3. Что такое периметровая защита сети, и как она помогает защищать веб-сервер?
4. Какие дополнительные меры защиты можно применять для фильтрации сетевых пакетов в Windows 2000?
5. Почему важно использовать зеркала дисков и дуплексирование для создания резервных копий, и какие у них ограничения?
6. Какое место в стратегии восстановления занимают резервные копии на съемных носителях?
7. Что такое экстренное восстановление, и как оно может помочь при сбоях системы?
8. Как создать загрузочные диски установки Windows 2000, и зачем они нужны?
9. Какие действия можно выполнить с помощью диска экстренного восстановления (ERD) в случае повреждения системы?
10. Что такое файл Setup.log, и какую информацию он содержит для восстановления системы?
11. Почему важно сохранять папку %systemroot%\Repair при установке Windows 2000, и что происходит при ее удалении?
12. Какую роль играют диски экстренного восстановления (ERD) при восстановлении паролей и учетных записей пользователей?
13. Какие файлы находятся на диске ERD и как они помогают в процессе восстановления системы?
14. Какие особенности настройки IIS для безопасного удаленного управления веб-сайтом должны быть учтены?
15. Какие шаги по созданию резервных копий и восстановлению системы следует предпринять для защиты веб-сайта от вирусных **атак и других угроз?**