**Лекции №14: Жизненный цикл управления безопасностью**

**Цель:** объяснить студентам основные этапы жизненного цикла управления безопасностью, начиная с планирования и оценки рисков, до реализации и мониторинга мер безопасности. Рассмотреть методы и практики, которые помогают обеспечивать безопасность на протяжении всего жизненного цикла систем и сервисов.

*Контроль безопасности* сайта представляет собой очень сложный процесс. Для успешного реагирования на нарушения безопасности необходим достаточно большой объем знаний. С помощью *структурного подхода* можно сделать этот процесс намного проще, что увеличит шансы на успех. В этой лекции мы расскажем о некоторых хорошо зарекомендовавших себя подходах к управлению безопасностью.

### Методология жизненного цикла

Жизненный *цикл управления* использует стандартизированный повторяемый набор процедур для обновления, переоценки и защиты сайта. Стандартизация обеспечивает правильную конфигурацию программного обеспечения, последовательное и предсказуемое выполнение задач. При помощи точно разработанных концепций политики обеспечивается эффективное реагирование. Схема жизненного *цикла* управления приведена на [рис. 7.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3529?page=1" \l "image.7.1).

Это очень важный подход, поскольку в динамической и изменяющейся среде интернета требуется *процесс управления*, постоянно адаптирующийся к возникающим ситуациям. Процесс укрепления системы основан только на фактах, о которых уже многое известно. Реализация жизненного *цикла* обеспечит переоценку подхода и *знание* тех изменений в технологиях, которые оказывают влияние на *сайт*.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/7/files/07_01.gif)

**Рис. 7.1.**Схема жизненного цикла управления

### Переоценка угроз и предупредительное отслеживание

Предупредительное отслеживание ограничивает попытки вторжений посредством периодической переоценки угроз. С точки зрения управления этот процесс выполняется на веб-сайте с целью своевременного обнаружения попыток вторжения и немедленного реагирования на возникшие угрозы. Отслеживание системы включает в себя регулярно проводимые обзоры журналов, а также более динамичные формы мониторинга с выводом уведомлений о потенциальных проблемах.

#### Переоценка угроз

Переоценка угроз представляет собой критический процесс, определяющий степень защищенности любой системы; этот процесс необходимо планировать как обычную процедуру управления безопасностью, так как в программно-аппаратных продуктах постоянно обнаруживаются все новые и новые слабые места. Программные продукты должны проверяться на стойкость к новым угрозам, выявляемым организациями типа института SANS после последних обновлений Microsoft.

Каждую систему нужно исследовать с помощью структурированного процесса, проверяющего текущее состояние защиты. Периодическая переоценка включает в себя мероприятия, описываемые в сводных перечнях этой книги и в других источниках информации о безопасности. Необходимо запускать новейшие средства безопасности, выпущенные Microsoft, для обработки всех возможных обстоятельств, связанных с безопасностью. Разумеется, средства, которые изначально использовались для повышения уровня безопасности (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)), обновляются Microsoft по мере обнаружения новые слабых мест.

Структурированный подход является ключом к успешной защите веб-сайта. Легко не выполнить какой-либо шаг или не завершить задачу, но вероятность таких ошибок уменьшится, если следовать упорядоченной схеме выполнения процесса. Ниже приведено краткое описание процесса переоценки.

* Примените последние исправления и процедуры по укреплению системы, имеющиеся в разделе безопасности веб-сайта Microsoft TechNet ([http://www.microsoft.com/technet/security](http://www.microsoft.com/technet/security" \t "_blank)). Так как эти исправления часто меняются, то здесь не указан конкретный адрес URL.
* Дважды проверьте основу безопасности сайта, запустив новое средство Microsoft Security Baseline Analyzer (MSBA) для проверки политики Windows 2000 и слабых мест в конфигурации, которые не были исправлены при помощи надстроек безопасности. Более подробную информацию об этой программе и инструкции по ее загрузке можно найти в документе Q320454 на сайте TechNet.
* Еще раз выполните IIS Lockdown, чтобы удостовериться в корректности конфигурации и политики безопасности IIS (см. ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521)).
* Проведите *тестирование безопасности* системы, настраивая основные параметры безопасности и применяя рекомендации в качестве превентивных мер защиты.
* Повторите этот цикл в соответствии с политикой безопасности организации.

##### Двойная проверка безопасности сервера

Программа Microsoft Baseline Security Analyzer (MBSA) предназначена для сканирования компьютеров с Windows 2000 и определения примененных в системе обновлений безопасности, политик безопасности и соответствующих параметров. MBSA представляет расширенную версию HFNetChk – широко известной программы, используемой многими системными администраторами Windows 2000. MBSA сканирует сервер для определения операционной системы, наличия сервис-пакетов и программ, после чего исследует базу данных Microsoft и определяет надстройки безопасности для установленного программного обеспечения.

MBSA, как и HFNetChk, проверяет создаваемые надстройкой ключи реестра и наличие на сервере определенной надстройки, а также выясняет версию и контрольную сумму каждого файла, установленного надстройкой. MBSA проверяет также соответствие настроек системы общим рекомендациям по безопасности сервера, например, устойчивость паролей, состояние учетной записи Guest (Гость), тип файловой системы, общедоступные файлы, группу администраторов, наличие распространенных ошибок в конфигурации. После выполнения процедуры генерируется отчет. Ниже приведен список проверок MBSA для сервера IIS.

* **Простые пароли**. MBSA в процессе сканирования проверяет компьютеры на наличие пустых, простых и неправильно указанных паролей:
  + пароль пуст;
  + пароль = имя пользователя (*имя учетной записи*);
  + пароль = имя компьютера;
  + пароль = "password";
  + пароль = "admin";
  + пароль = "Administrator".
* **Группа Administrators** (Администраторы). Определяет и создает перечень учетных записей, принадлежащих группе Local Administrators (Локальные администраторы). При обнаружении более двух учетных записей администраторов программа выводит список их имен и обозначает потенциальное слабое место. Рекомендуется свести к минимуму число администраторов, так как они по природе своей деятельности осуществляют полный контроль над системой.
* **Аудит**. Определяет включение аудита на сканируемом компьютере. Аудит Microsoft Windows отслеживает и фиксирует в журнале определенные *системные события*, такие как успешные и неудачные попытки входа в систему. Следует всегда вести журнал и отслеживать события системы, чтобы определять потенциальные угрозы безопасности и вредоносные действия.
* **Автоматический вход в систему**. Определяет включение автоматического входа, наличие шифрования пароля входа в реестре или хранение его в открытом виде. Если включен автоматический вход в систему, и пароль хранится в открытом виде, это будет отражено в отчете безопасности как серьезное слабое место. Если включен автоматический вход, и пароль шифруется в реестре, это будет отражено в отчете безопасности как потенциальное слабое место.
* **Проверка наличия ненужных служб**. Определяет включение служб, содержащихся в текстовом файле services.txt. Если планировалось отключение какой-либо службы, но этого не произошло, или служба перезапустилась, то данная проверка выявит этот факт.
* **Гостевая учетная запись**. Определяет включение встроенной учетной записи Guest (Гость). Гостевая учетная запись используется для входа на компьютер с ОС Windows 2000 и должна быть отключена.
* **Виртуальные каталоги MSADC и Scripts на сервере IIS**. Определяет установку виртуальных каталогов MSADC (образцы сценариев доступа к данным) и Scripts. Сценарии в этих каталогах нужно удалить для снижения вероятности проведения атаки.
* **Виртуальный каталог IISADMPWD**. Определяет установку виртуального каталога IISADMPWD. В IIS 4.0 пользователи могут через него изменять свои пароли. IISADMPWD является слабым местом, через которое возможно раскрытие паролей. При обновлении сервера до IIS 5 этот каталог нужно удалить,
* **Средство IIS Lockdown**. Определяет выполнение на компьютере версии 2.1 программы IIS Lockdown. IIS Lockdown отключает ненужные возможности и настраивает политику безопасности IIS для уменьшения степени уязвимости защиты.
* **Журнал IIS**. Определяет включение журнала IIS и использование расширенного формата файла журнала W3C. Ведение журнала IIS выходит за рамки функций Windows и позволяет обнаружить возможные области атаки сервера или сайтов. Эта возможность должна быть всегда включена.
* **Родительские пути IIS**. Определяет включение параметра ASPEnableParentPaths. При включении родительских путей на страницах Active Server Pages (ASP) используются *относительные пути* от текущего каталога к домашнему каталогу (пути, использующие символ "..").
* **Демонстрационные приложения IIS**. Определяет установку на компьютере папок с демонстрационными файлами:
* \Inetpub\iissamples
* \Winnt\help\iishelp

\Program Files\common files\system\msadc

Эти каталоги и все виртуальные каталоги нужно удалить.

* **Члены роли Sysadmin (Системный администратор)**. Определяет число членов роли *Sysadmin* и отображает результаты в отчете безопасности. Как правило, в роли *Sysadmin* должно содержаться как можно меньше пользователей.
* **Окончание срока действия пароля**. Определяет наличие в учетных записях локального пользователя пароля с неограниченным сроком действия. Пароли должны регулярно меняться для предотвращения атак на взлом паролей. Такие учетные записи будут указаны в отчете.
* **Ограничение анонимных пользователей**. Определяет использование ключа реестра RestrictAnonymous для ограничения анонимных подключений разрешениями Read (Чтение) или Read and Execute (Чтение и выполнение) в каталогах сценариев (если они имеются).
* **Общие объекты**. Определяет наличие общих папок. В отчете будут показаны все найденные на компьютере общие объекты, включая администраторские общие папки, а также их разрешения уровня общего доступа и уровня NTFS. На веб-сервере ни в коем случае не должны присутствовать общие папки!

Перед запуском MBSA следует уяснить две вещи. Во-первых, проверка входа вызовет создание записей в журнале событий безопасности, если на компьютере включен аудит событий входа/выхода из системы. Во-вторых, тест на ненужные службы использует файл services.txt в качестве *контрольного списка*. Отредактируйте этот файл таким образом, чтобы он содержал конкретные службы для проверки на каждом сканируемом компьютере. Файл services.txt, устанавливаемый по умолчанию с этой программой, содержит следующие службы:

MSFTPSVC (FTP)

TlntSvr (Telnet)

RasMan (Диспетчер службы удаленного доступа)

W3SVC (WWW)

SMTPSVC (SMTP)

Перечень остальных служб, которые необходимо отключить, см. в ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521).

##### Тестирование на уязвимость в реальном режиме

Специалисты в области информационной безопасности рекомендуют проводить тестирование в реальном режиме для проверки воздействия атак, посредством которых хакеры определяют степень защищенности веб-сайта. В статье "Переоценка уязвимости: превентивные меры по обеспечению безопасности вашей организации", опубликованной на веб-сайте SANS, говорится, что при проведении переоценки уязвимых мест используемый набор средств должен быть похож на тот набор инструментов, который использует противник. Это обеспечит защищенность систем от атак, которые в данный момент находятся на пике популярности среди хакеров.

Ниже приведен список некоторых полезных средств, которые можно бесплатно загрузить из интернета. Коммерческое программное обеспечение для сканирования выпускается такими производителями как Symantec, Network Associates, BindView, eDigital Security и *Internet Security* Systems.

* **Nmap** – утилита для исследования сети и/или аудита безопасности. Быстро и аккуратно сканирует сети и определяет доступные узлы, работающие службы и используемые операционные системы. Доступна по адресу [http://www.insecure.org](http://www.insecure.org/" \t "_blank).
* **Nessus** – удаленный сканер безопасности. Осуществляет аудит сети и определяет наличие уязвимых мест. Программа запускает имеющиеся в ее комплекте эксплоиты и выводит отчет о степени успеха работы каждого из них. Доступна по адресу [http://www.nessus.org](http://www.nessus.org/" \t "_blank).
* **Whisker** – интернет-сканер CGI. Осуществляет сканирование на предмет наличия известных уязвимых мест в веб-серверах с предоставлением URL, вызвавшего событие. Определяет тип функционирующего веб-сервера, легко обновляется и имеет множество полезных возможностей. Доступна по адресу [http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2](http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2" \t "_blank).
* **Enum** – консольная Win32-утилита для сбора информации. С помощью недействительных сеансов получает перечни пользователей, компьютеров, общих объектов, имен, групп и членов групп, а также информацию о паролях и политике. Осуществляет примитивную атаку грубой силы, направленную на отдельные учетные записи. Доступна по адресу [http://razor.bindview.com/tools/index.shtml](http://razor.bindview.com/tools/index.shtml" \t "_blank).

Некоторые из этих средств работают под Windows, некоторые – под UNIX или Linux. Если вы немного разбираетесь в хакерстве, имеете доступ к платформам, использующим отличную от Windows платформу, и достаточно времени для тестирования, то сможете самостоятельно выполнить нужные тесты для подтверждения защищенности сервера. Однако большинство из вас не сможет этого сделать.

Существует альтернативный подход. Один из вариантов – обращение к консультанту. Также можно использовать новый, доступный в интернете, тип служб, осуществляющий автоматическое сканирование сайта. Выполнив поиск в системе Google по строке "Online *Vulnerability* Testing Service", вы получите перечень компаний, предлагающих подобные услуги. Некоторые из этих услуг имеют бесплатные демонстрационные версии, и вам стоит потратить время на их изучение.

**Вопросы для закрепления:**

1. Что включает в себя жизненный цикл управления безопасностью и почему его стандартизация важна для успешной реализации мер безопасности?
2. Как процесс переоценки угроз способствует улучшению безопасности системы?
3. Какие шаги необходимо выполнить в рамках переоценки угроз для укрепления системы?
4. Что такое Microsoft Baseline Security Analyzer (MBSA) и как он помогает в обеспечении безопасности?
5. Какие основные уязвимости проверяет MBSA на сервере IIS?
6. Какие рекомендации дают эксперты по ограничению числа администраторов и как это влияет на безопасность?
7. Что такое тестирование на уязвимость в реальном времени и как оно помогает повысить безопасность веб-сайта?
8. Какие инструменты можно использовать для сканирования безопасности сети и какие их особенности?
9. Какую роль играет регулярное обновление программного обеспечения в процессе обеспечения безопасности?
10. Какие основные принципы соблюдаются при проведении тестирования на уязвимость с использованием таких инструментов, как Nmap и Nessus?