**Лекция №9: Удаление, повреждение и отказ в доступе к данным**

**Цель: и**зучить способы удаления, повреждения и отказа в доступе к данным, а также их влияние на информационную безопасность. Ознакомить студентов с методами защиты данных от этих угроз и с практическими подходами для предотвращения потери или повреждения информации в организациях.

Слабые места сайта возникают при неправильной конфигурации сервера или в случае нехватки знаний в области безопасности у веб-администратора. Тем не менее, эти недостатки легко устраняются. Иногда "брешь" появляется из-за недостаточно четкого планирования защиты, ошибки в программном обеспечении, либо она заложена в самой природе протоколов интернета. Устранение этих проблем требует глубокого понимания связанных с ними вопросов. В данной лекции рассказывается об известных уязвимых местах *IIS*, об их использовании при выполнении атак на серверы Microsoft *IIS*.

### Источник проблемы

Веб-*сайт* подвергается атакам на взлом по ряду причин. Одной из причин является то, что коммерческое *программное обеспечение*, на котором построены веб-сайты, представляет собой сложные и комплексные платформы. Как и любое другое, оно иногда содержит ошибки ("баги"), которые и используются взломщиками. Другая причина заключена в самой технологии *интернет*-протоколов, согласно которой функционирует вся *сеть* *интернет*. При их создании изначально не учитывались вопросы безопасности. *Интернет*-протоколы появились в результате нововведений, усовершенствований, совместных разработок в области информационных технологий, выполняемых в научно-исследовательских институтах, группах индустриальных стандартов и на частных предприятиях, чтобы открыть *доступ* к информации большому количеству людей. Целью этих технологий было *объединение* людей, а не их разграничение.

Несмотря на то, что впоследствии были разработаны способы обеспечения безопасности *интернет*-протоколов, их *архитектура* в общем и целом осталась уязвимой, а *затраты* на усиление информационной безопасности порой превышают *затраты* на введение новой архитектуры.

Открытая и единая природа протоколов интернета явилась одной из главных причин его небывалой популярности. Они стали настоящими стандартами, благодаря чему продукты от различных производителей взаимодействуют на удивление слаженно. К сожалению, из-за наличия проблем с их безопасностью разработчики программного обеспечения вынуждены время от времени совершенствовать свои продукты. На рынке появилось новое направление программных средств, предназначенных для обеспечения безопасности информации. Многие компании широко применяют эти средства для достижения наилучших результатов в области защиты своих систем.

### Понятие протокола интернета

Давайте вначале ознакомимся с кратким описанием протоколов интернета. Работа интернета основана на функционировании набора специализированных *коммуникационных протоколов*. В [таблице 2.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3519?page=1" \l "table.2.1) приведены некоторые протоколы и их описание, к которым мы будем возвращаться при работе со следующими лекциями. Если вы уже знакомы с работой сетей *TCP*/*IP* и технологиями World Wide *Web*, можете пропустить эту тему и перейти к следующему параграфу.

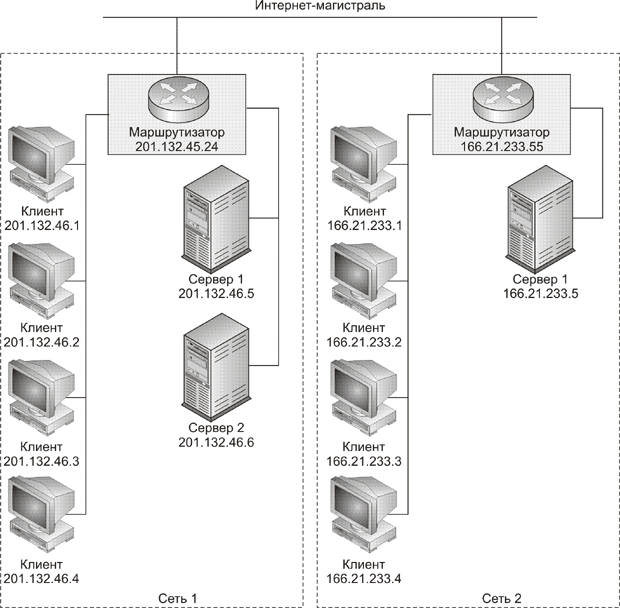
|  |  |
| --- | --- |
| Таблица 2.1. Основные протоколы TCP/IP | |
| **Протокол** | **Описание** |
| Internet Protocol (IP) | Используется для управления инфраструктурой и присвоения компьютерам адресов, уникальным образом идентифицирующих каждый узел числом, состоящим из идентификаторов сети и узла. IP-адрес может выглядеть так: 192.168.222.101. |
| Internet Control *Message Protocol* (ICMP) | Обеспечивает механизм передачи сообщений об ошибках в протоколе IP на узел, сгенерировавший IP-пакет; используется для уведомления об ошибках, возникших при передаче данных. |
| Dynamic Host Control Protocol (DHCP) | Разрешает динамическое присвоение IP-адресов узлам в контролируемой подсети для устранения поддержки фиксированного IP-адреса каждого узла. |
| Transmission Control Protocol (TCP) | Управляет коммуникационными действиями между процессами в объединенных узлах, работающих независимо от инфраструктуры, управляемой протоколом IP. |
| User Datagram Protocol (UDP) | Является альтернативой TCP, используется для передачи данных между процессами, не требующими надежной доставки по причине того, что процессы самостоятельно исправляют ошибки. |
| File Transfer Protocol (FTP) | Простой и надежный протокол для обмена файлами между узлами. |
| Point-to-Point Protocol (PPP) | Обеспечивает надежную связь и набор опций для автоматизации процессов входа в систему и настройки удаленных узлов. |
| Simple Mail Transfer Protocol (SMTP) | Используется для передачи исходящих сообщений электронной почты с одного узла на другой. |
| *Post Office Protocol* (POP) | Используется для передачи входящих сообщений электронной почты с одного узла на другой. |
| Simple *Network Management* Protocol (SNMP) | Используется в процессе управления сетью при сборе данных для анализа и составления отчета о производительности сетей. |
| *Hypertext Transfer Protocol* (HTTP) | Используется веб-браузерами и веб-серверами для осуществления запросов и отправки содержимого в формате HTML. |

Приведенные протоколы *TCP*/*IP* определяют набор стандартов, используемых разработчиками программного обеспечения для обмена данными между двумя компьютерами. Это позволяет программным приложениям правильно осуществлять доставку данных. Каждый протокол играет свою собственную роль при обмене информацией.

### Протоколы интернета

Аббревиатура "*IP*" является сокращением от *Internet Protocol* (Протокол интернета), т.е. от названия одного из протоколов *TCP*/*IP*. Его роль заключается в идентификации компьютеров (называемых узлами или хостами), между которыми производится *обмен данными*.

Протокол *Internet Control Message Protocol* (*ICMP*) функционирует параллельно протоколу *IP* и позволяет маршрутизаторам отправлять сообщения друг другу для определения оптимального и надежного пути от одного компьютера к другому в сложнейшей среде глобальной сети. На [рисунке 2.1](https://www.intuit.ru/studies/courses/1002/122/lecture/3519?page=1" \l "image.2.1) приведена схема инфраструктуры интернета и показан принцип *IP*-адресации.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/2/files/02_01.gif)

**Рис. 2.1.**Протоколы интернета позволяют системам обмениваться информацией независимо от их физического расположения

Протоколы *Transmission Control Protocol* (*TCP*) и *User Datagram Protocol* (*UDP*) (в меньшей степени) используются для управления транспортировкой данных между двумя компьютерами. С их помощью открываются и закрываются соединения, доставляются и верифицируются данные при обмене информацией.

#### Доменная система имен

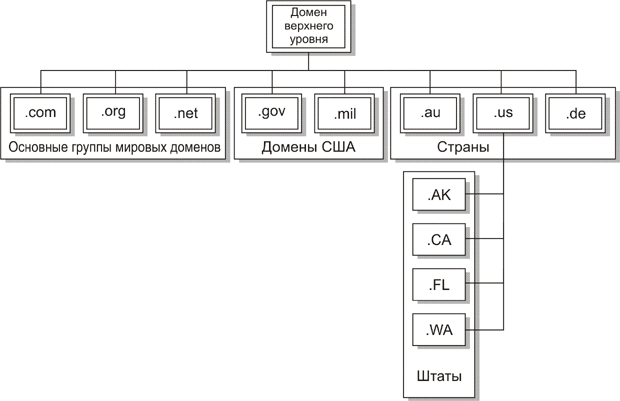
Сеть интернет чрезвычайно велика, а вид IP-адреса пугает пользователей (хотя форма адреса является стандартной для компьютеров), поэтому требуется некоторая централизованная служба для успешного нахождения требуемых компьютеров. Централизованная служба имен (Domain Name System, DNS) позволяет пользователям находить информацию и отправлять сообщения электронной почты с использованием понятного для людей языка. С помощью DNS можно открыть сайт своей библиотеки, введя в веб-браузере адрес *URL* (Universal Resource Locator), например, **www.mylibrary.com**, вместо малоинформативного адреса 196.221.68.124. Можно отправить сообщения электронной почты на santa@northpole.org вместо 64.230.64.121@232.110.98.101.

**Совет**. Имена доменов в Соединенных Штатах Америки контролируются некоммерческой организацией *ICANN* (Internet Corporation for Assigned Names and Numbers), являющейся полугосударственной структурой. Она также называется InterNIC. В Европе и Азии имеются собственные системы управления доменными именами.

Служба доменных имен отслеживает информацию, необходимую для поиска какой-либо системы, чтобы это не выполнял каждый отдельно взятый компьютер. *Служба DNS* организована в иерархию, обеспечивающую эффективность и скорость поиска адресов (см. [рис. 2.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3519?page=2" \l "image.2.2)). На вершине располагается *домен верхнего уровня* (Top Level Domain, *TLD*). Все остальные домены (.com, .net и .org) ответвляются от домена верхнего уровня.

#### Приложения и службы

При информационном обмене требуются различные протоколы передачи-приема данных. Например, при обмене данными интернета используется протокол HTTP (*Hypertext Transfer Protocol*), клиенты электронной почты используют протокол *SMTP (Simple Mail Transfer Protocol*), а обмен файлами – протокол FTP (File Transfer Protocol). Программные приложения, такие как веб-браузер, клиент электронной почты или клиент FTP, передают данные в формате тех протоколов, посредством которых происходит обмен информацией.

[](https://www.intuit.ru/EDI/27_04_15_5/1430086749-14056/tutorial/221/objects/2/files/02_02.gif)

**Рис. 2.2.**Иерархическая структура системы доменных имен DNS

Каждый компьютер в сети интернет теоретически может быть связан напрямую с другим компьютером, но на самом деле интернет работает по-другому. Компьютеры используют веб-браузер или программу электронной почты и взаимодействуют с серверами, на которых работают соответствующие службы приложений: веб-сервер HTTP, сервер электронной почты SMTP, сетевые службы FTP (общий доступ к файлам) и Telnet (удаленные терминалы). На многих серверах выполняются одновременно несколько служб приложений. Поэтому программное обеспечение для интернета использует набор портов, идентифицируемых по номерам в диапазоне от 1 до 65535. Номера портов позволяют операционной системе сервера управлять несколькими приложениями или сетевыми службами, а также клиентскими соединениями в каждой службе. Службы HTTP обычно используют порт 80, службы SMTP – порт 25, службы FTP – порты 20 и 21. Более подробный, но далеко не полный, перечень служб приведен в [табл. 2.2](https://www.intuit.ru/studies/courses/1002/122/lecture/3519?page=2" \l "table.2.2).

Пакет протоколов интернета содержит около ста наименований. Здесь же приведены только общие сведения, необходимые для последующего изучения материала.

|  |  |  |  |
| --- | --- | --- | --- |
| Таблица 2.2. Основные порты приложений | | | |
| **Служба** | **Используемый порт** | **Транспортировка** | **Функция** |
| FTP | 21 | TCP | Передача файлов. |
| Telnet | 23 | TCP | Удаленные терминалы. |
| SMTP | 25 | TCP | Исходящая почта. |
| Служба имен (DNS) | 53 | UDP | Списки имен интернета. |
| HTTP | 80 | TCP | Сеть. |
| POP | 109, 110 | TCP | Входящая почта. |
| Программа удаленного контроля (*RCP*) | 111 | TCP и UDP | Удаленное выполнение программ. |
| Сетевой протокол передачи новостей (NNTP) | 119 | TCP | Списки новостей интернета. |
| Сетевой протокол времени (*NTP*) | 123 | UDP | Синхронизация времени. |
| NetBIOS (Win NT) | 135, 139, 137, 138 | TCP, UDP | Сетевые подключения Windows (не TCP/IP). |
| NetBIOS (Win2000) | 135, 139, 137, 138, 445 | TCP и UDP | Сетевые подключения Windows (не TCP/IP). |
| Протокол доступа к сообщениям в сети интернет (IMAP) | 143 | UDP | Почтовый протокол. |
| SNMP | 161, 162 | TCP и UDP | Управление сетью. |
| Пограничный сетевой протокол (*BGP*) | 179 | TCP | Управление пограничным шлюзом |
| Облегченный протокол службы каталогов (LDAP) | 389 | TCP и UDP | Службы каталогов. |
| Протокол защищенных сокетов (SSL) | 443 | TCP | Защищенные, зашифрованные данные сети. |
| *Системный журнал* | 514 | UDP | Сетевой журнал. |
| "Демон" линейного принтера (LPD) | 515 | TCP | *Сервер печати* (UNIX). |
| *SOCKS* | 1080 | TCP | Сетевой прокси-сервер. |

### Известные уязвимые места

Институт системного администрирования, сетевых подключений и безопасности (SANS) включает в себя более чем 90 000 системных администраторов, профессионалов в области безопасности и сетевых администраторов, что делает данную организацию наиболее заметной структурой, занимающейся безопасностью интернета. Члены SANS публикуют свои исследования, различные статьи, учебные пособия и новости, обмениваясь информацией друг с другом и с общей массой пользователей.

Каждый год институт SANS составляет перечень наиболее опасных угроз, которым подвержены компьютеры и *компьютерные сети*. Этот перечень носит название "The Twenty *Most* *Critical* *Internet* *Security Vulnerabilities*" ("Двадцать наиболее опасных угроз безопасности в интернете") или "The SANS/*FBI* *Top* 20". Он разрабатывается на базе многолетнего опыта, знаний, среднестатистических сведений, получаемых с помощью совместных исследований. Перечень постоянно обновляется, он находится по адресу [http://www.sans.org/top20.htm](http://www.sans.org/top20.htm" \t "_blank). Он содержит сведения об угрозах, представляющих опасность для всех систем, и об уязвимых местах, присущих только системам Microsoft. Большинство уязвимых мест Microsoft *IIS* устраняется после установки сервис-пакетов или *патчей* безопасности.

В следующем разделе содержится сокращенный вариант перечня SANS с описанием проблем и набором дополнительных сведений. Раздел "*Переполнение буфера*" содержит информацию с веб-сайта Symantec ([http://www.Symantec.com](http://www.symantec.com/" \t "_blank)).

#### Общие уязвимые места

Некоторые уязвимые места в защите являются общими для всех информационных систем. Например, любая система, использующая парольную защиту, подвержена атакам при небезопасной работе с паролями. Поэтому, независимо от того, используется ли Windows или UNIX, веб-сервер имеет следующие слабые места.

##### Заданные по умолчанию настройки операционных систем и приложений

Большая часть программного обеспечения, включая операционные системы и приложения, поставляется с инсталляционной программой, автоматически копирующей и настраивающей его на компьютере. Однако инсталляционные программы зачастую устанавливают большее число компонентов, чем требуется. Многие администраторы не знают об этом, что приводит к появлению "дыр" в программном обеспечении их компьютерных систем.

При инсталляции приложений часто устанавливаются ненужные демонстрационные программы и сценарии. При установке операционной системы почти всегда инсталлируются дополнительные службы и соответствующие им открытые порты. Через эти порты злоумышленники и проникают в систему.

Одним из наиболее уязвимых мест в защите веб-сервера являются демонстрационные сценарии, которые используются злоумышленниками для несанкционированного доступа в систему или для получения информации о системе. Демонстрационные сценарии, как правило, не проходят контроля качества, которому подвергается другое программное обеспечение. В результате они становятся прекрасной целью для атак, вызывающих переполнение отведенной сценарию оперативной памяти, что позволяет злоумышленнику внедрить свою собственную программу в память и выполнить ее.

Решение этой проблемы, включающее в себя закрытие портов и удаление демонстрационных сценариев, является частью процесса, называемого *усилением системы*. Этот процесс будет детально обсуждаться в ["Подготовка и укрепление веб-сервера"](https://www.intuit.ru/studies/courses/1002/122/lecture/3521).

**Вопросы для закрепления:**

1. В чем заключается основная угроза при неправильной конфигурации веб-сервера?
2. Почему уязвимости в интернет-протоколах считаются системными, а не просто ошибками программного обеспечения?
3. Каковы причины того, что интернет-протоколы изначально не учитывали вопросы безопасности?
4. Назовите основные протоколы TCP/IP и кратко опишите их назначение.
5. Что такое ICMP и какую роль он играет в инфраструктуре интернета?
6. Почему DNS-система необходима для работы интернета?
7. В чем преимущества и недостатки открытой архитектуры интернет-протоколов?
8. Как назначение портов помогает управлять сетевыми службами на одном сервере?
9. Перечислите уязвимости, характерные для Microsoft IIS.
10. Что такое «усиление системы» и какие шаги оно включает?
11. Как демонстрационные сценарии и лишние службы могут угрожать безопасности сервера?
12. Почему переполнение буфера считается критической уязвимостью?
13. Что такое «SANS/FBI Top 20» и как он используется специалистами по ИБ?
14. Почему важно своевременно устанавливать обновления и патчи для ПО?
15. Как динамическое присвоение IP-адресов (DHCP) влияет на безопасность сети?
16. Объясните роль протокола TCP в обеспечении надежности передачи данных.
17. Какие существуют способы отказа в доступе к данным и как их предотвращать?
18. Чем отличается протокол UDP от TCP с точки зрения надежности?
19. Почему важно ограничивать и контролировать установленные сетевые службы?
20. Каковы последствия атаки на DNS и как защитить доменную систему?