

Шабунь В.С., студент 437 гр.

Научный руководитель — Петренко Б.В.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИБЛИОТЕЧНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Она, являясь системообразующим фактором жизни общества, активно влияет на состояние всех сфер жизни. Информационные технологии вошли в нашу жизнь, и обойтись без них мы уже не можем. Сегодня информация — важный, стратегический ресурс, который влияет на нашу жизнь. Информация и информационные технологии могут быть направлены на благо, или же использованы во вред. Информационная безопасность занимает многие умы, как обычных людей, так и на государственном и международном уровне. Для обеспечения информационной безопасности нужно исследовать эту область. Методы незаконного воздействия на информацию и информационные системы развиваются с каждым днём. Поэтому в мире создаются самые современные системы безопасности информации. Сегодня компьютерные сети являются важным элементом функционирования компьютерной среды. Они связывают между собой пользователей в одну сеть для передачи информации. Так как компьютерные сети сегодня развиты, существуют способы на их посягательства.

Вопросами защиты информации занимались такие учёные и их публикации как Л.И. Алёшин «Безопасность в библиотеке», В. В. Арутюнов «Основы информационной безопасности», А.А. Грушо «Теоретические основы защиты информации», Г.А. Атаманов

«Информационная безопасность: сущность и содержание», А.Д. Урсул «На пути к устойчивому развитию цивилизации: информационные факторы», В.Я. Асанович «Информационная безопасность. Анализ и прогноз информационного воздействия» и т.д.

Компьютерная сеть – это комплекс аппаратных и программных средств, позволяющих осуществлять связь между компьютерами, получать и передавать данные, решать задачи общения, совместно использовать компьютерные ресурсы.

Локальная сеть: обеспечивает наивысшую скорость обмена информацией между компьютерами. Типичная локальная сеть занимает территорию в несколько зданий. Протяжённость локальных компьютерных сетей достигает всего лишь несколько километров.

Глобальная сеть: позволяет организовать взаимодействие между компьютерами на огромных расстояниях. Эти сети работают на относительно низких скоростях и могут вносить значительные задержки в передачу информации. Протяжённость таких сетей может составлять тысячи километров.

Выделяются такие локальные сети как: одноранговые и клиент-сервер. Одноранговые компьютерные сети — компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов.

Клиент-сервер — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами. Фактически клиент и сервер — это программное обеспечение.

Обычно эти программы расположены на разных вычислительных машинах и взаимодействуют между собой через вычислительную сеть посредством сетевых протоколов, но они могут быть расположены также и на одной машине

Далее можно рассмотреть виды угроз компьютерным сетям и средства защиты такие.

Угрозы компьютерной сети делятся на активные и пассивные

К активным угрозам относятся:

- отказ служб передачи сообщений – злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;
- «маскарад» – злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;
- внедрение сетевых вирусов – передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;
- модификация потока сообщений – злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Среди пассивных угроз выделяют:

- просмотр сообщения;
- анализ графика – злоумышленник может просматривать заголовки пакетов, циркулирующих в сети, и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности, длина сообщения, объем трафика и т.д.).

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы. К сервисам безопасности относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование, антивирусные программы, средства архивации данных.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством *аутентификации* вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

Криптография – наука о методах обеспечения конфиденциальности и аутентичности информации. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Процесс *шифрования* заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования информации используются алгоритм преобразования и ключ.

Функционирование компьютерных сетей и обеспечение информационной безопасности, на примере Белорусского

государственного университета культуры и искусств. Сеть выстроена в топологию «звезда». Имеется 9 серверов модели SuperMicro. Длина сети приблизительно 20 км. Используется файловое хранилище Кинап. Установлены управляемые коммутаторы Planet D-Link. Скорость передачи данных внутри сети 1Гбит.с. Безопасность обеспечивается:

- 1) Антивирусом Касперского 10 версия.
- 2) Пользователи не имеют никаких прав. Все права находятся у системных администраторов.

Все вышеперечисленные виды угроз и средства защиты информации в компьютерных сетях, являются основой их функционирования. Информационные технологии интенсивно развиваются, а также вместе с ними и развиваются методы посягательства на целостность информации.

1. Безопасность компьютерных сетей : [учебное пособие] / В.Г. Олифер, Н.А. Олифер. – Москва: Горячая линия-телеком, 2014.- 643с.

2. Бирюков А.А. Информационная защита. Защита и нападение/ А.А. Бирюков.- Москва: ДМК Пресс, 2012.- 474с.

3. Богущ, В.А. Компьютерные сети: курс лекций/ А.В. Богущ, И.С. Терех, Министерство образования Республики Беларусь, учреждение образования Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГЭУ, 2006. – 104с.

4. Бони, Джеймс. Руководство по Cisco IOS для профессионалов = Cisco IOS in a Nutshell : [полное описание команд] / Дж. Бони ; [пер. с англ. Е. Шикарева]. - [2-е изд.]. - Москва : Русская Редакция ; Санкт-Петербург : Питер, 2007. – 784 с. : ил.

5. Борщев,Б.В. Интернет и информационная среда / Б. В. Борщев// Научно-техническая информация. Серия 2, Информационные процессы и

системы. – 2009. – № 2. – С. 1-14. – (Общий раздел). – Библиогр.: с. 14 (15 назв.).

Шамарова Е.В., Космич В.С., студ. 202 гр.
Научный руководитель – Лещенко Н.В.

КОНСПИРОЛОГИЧЕСКОЕ СОЗНАНИЕ АМЕРИКАНЦЕВ

Вера в заговор, оккультные силы и могущественные тайные организации, в «невидимую руку» и «мировую закулису», незримо управляющую ходом истории и подчиняющую народы и государства злой воле законспирированных «тайных господ», существовала в человечестве всегда. В виду такой значимости подобных явлений сформировалась такая наука как конспирология, которая представляет собой совокупность гипотез, которые пытаются объяснить последовательность общественно значимых событий, определенные исторические явления, или ход истории в целом как результат заговора со стороны некоторой группы людей, управляющих этим процессом из корысти, амбиций или иных групповых, клановых и других интересов [2, с.7].

Самая популярная теория заговора, что составляет большой процент конспирологического сознания американского населения – тайное общество Иллюминатов. Ученые также утверждают, что данная тайная организация существовала на протяжении двух тысяч лет, при этом часто меняла свои названия, чтобы не привлекать лишнего внимания людей и запутать следы. Никто из тех, кто был иллюминатом, не говорил об этом открыто, поскольку за это грозила смерть. Все иллюминаты очень дорожили собственной жизнью, даже несмотря на то, что знали о множестве воплощений.