Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Санкт-Петербургский национальный исследовательский  
университет информационных технологий, механики и оптики»

**Мегафакультет: К**омпьютерных технологий и Управления

**Факультет:** Информационной безопасности и компьютерных технологий

**Кафедра:** Проектирования и безопасности компьютерных систем

**Направление (специальность)** «Информационная безопасность»

**Профиль** 10.03.01 «Комплексная защита объектов информатизации»

**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

По дисциплине:

«**Основы информационной безопасности**»

На тему:

«Специфические особенности защиты информации в локальных и глобальных компьютерных сетях»

**Выполнили:**

cтуденты гр.3164

Смирнов Максим

Боязитов Артём

Плешаков Илья

**Преподаватель:**

Сухостат В. В.

**Количество баллов:\_\_\_\_\_\_\_\_\_\_\_\_**

**Дата защиты: «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2017г.**

Введение 3

Цель 4

Терминология 5

Точки защиты 6

Клиентские рабочие станции 6

Веб-сервер. 8

Шлюзы. 9

Заключение 12

# Введение

Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

По данным Миннесотского университета США, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули свой бизнес, причем половина из них заявила о своей несостоятельности немедленно.

# Цель

Проанализировать базовую систему защиты операционныой системы ПК, работающего как звено интерсети. Выявить уязвимые и плохо защищенные места и предложить алгоритмы защиты, организационные, программные, аппаратно-программные средства защиты.

# Терминология

|  |  |
| --- | --- |
| Аутентификация | Проверка идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед выдачей разрешения на доступ). |
| Авторизация | Предоставление субъекту прав на доступ к объекту. |
| Безопасность информации | Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования. |
| Доступ | Специальный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому. |
| Пароль | Идентификатор субъекта системы, который является его (субъекта) секретом |
| Политика безопасности | Набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение защищаемой информации в системе. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. |

# Точки защиты

## Клиентские рабочие станции

Браузеры - основные, но не единственные пункты защиты клиента в интрасети. Они могут оказаться не более защищенными, чем операционные системы и рабочие станции, на которых запускаются эти браузеры. Если исходить из традиционных критериев, предъявляемых к информационным системам, то современные Web-браузеры - очень уязвимые клиентские приложения. Как отмечает Харт, браузеры, предлагаемые для массового рынка, не имеют функций защиты, необходимых для поддержки критически важных приложений интрасети. Среди самых уязвимых мест современных коммерческих браузеров - отсутствие защиты паролем, неограниченный доступ к локальным ресурсам компьютера и возможность раскрытия критически важных данных при помощи кнопок "вперед/назад", закладок и выделенных цветом ссылок.

По словам Бреда Джонсона, руководителя фирмы SystemExperts, консультирующей по вопросам защиты, опытные пользователи "обходят" уязвимые места, реализуя клиентские приложения, которые имеют функции защиты. "Многие разработчики приложений для интрасетей решили, что будет неплохо ужесточить требования к клиентам, чтобы гарантировать управляемость и защиту своих Web-транзакций, - говорит Джонсон. - Среди этих дополнений - подключаемые к браузеру модули, браузеры, имеющие функции защиты, и клиенты, предназначенные для конкретного приложения".

Многие считают, что браузеры и рабочие станции, на которых они установлены, имеют вполне достаточную защиту, а вот intranet- и Internet-соединения доверия не внушают. Чтобы снять этот вопрос, в большинстве коммерческих браузеров была реализована поддержка версий протокола шифрования Secure Sockets Layer (SSL) 2.0 и 3.0, предназначенных для защиты транзакций, которые осуществляются в соответствии с HTTP, FTP и другими протоколами Internet. SSL использует шифрование с открытым ключом для обмена в одном сеансе 40- или 128-разрядным ключом между браузером и Web-сервером. Ключ сеанса применяется для шифрования как запроса, так и ответа при интерактивной транзакции; личные ключи пользователя и сервера сохраняются в секрете.

Аутентификация и возможности шифрования в SSL довольно выразительны, но ненадежны. Как показали исследования, современные вычислительные средства позволяют преодолеть защиту поддерживающих SSL браузеров, таких как Netscape Navigator. Некоторые эксперты считают SSL недостаточно надежным для поддержки интенсивной электронной коммерции. "Нельзя использовать в корпоративной среде 40-разрядные ключи для чего-то более важного, чем общедоступная информация, - считает Энтони Нельсон, президент ESTec Systems, консалтинговой компании, занимающейся вопросами защиты информации. - Даже 128-разрядный ключ в коммерческом сервере не адекватен для приложений, которые управляют критически важной информацией или большими денежными средствами".

Тем не менее далеко не все администраторы сети обеспокоены уровнем безопасности SSL - во всяком случае, не больше, чем они озабочены загрузкой пользователями злонамеренных аплетов Java или управляющих элементов ActiveX. Защита интрасети во многом зависит от того, можем ли мы доверять программным компонентам (аплетам, управляющим элементам, подключаемым модулям и другим исполняемым компонентам), которые браузеры постоянно загружают и устанавливают повсюду.

Что касается Java, многие считают его самым безопасным. Базовая модель защиты Java, называемая "песочницей" (sandbox), не разрешает аплетам чтение и запись на диски пользовательских ПК, а также взаимодействие с любым Web-сервером, кроме того, где эти аплеты инициированы. Наоборот, элементы управления ActiveX обычно имеют доступ к сетевым и локальным (компьютера пользователя) ресурсам, поэтому потенциально могут нанести большой вред. "Нам пришлось несколько раз проводить оценку Java и ActiveX, сравнивая различные аспекты защиты. В каждом случае мы признавали поражение ActiveX, - говорит Нельсон из ESTec Systems. - Даже в относительно управляемой корпоративной интрасети риск заражения вирусами и мошенничества с кодом в приложениях ActiveX слишком велик".

Однако, модель защиты "песочница" была существенно ослаблена при реализации в Netscape Communicator и других ориентированных на SSL браузерах. Не исключено, что в скором времени Java станет во многих практических приложениях не более надежным, чем ActiveХ. Пользователи смогут конфигурировать Communicator для предоставления доверенным аплетам Java привилегий, которыми обладают элементы управления ActiveХ, - например, возможности доступа к другим узлам Web, чтения и записи на локальный или сетевой диск. Чтобы получить эти привилегии, аплеты должны быть "подписаны", т. е. содержать цифровые сертификаты от доверенных издателей информационного наполнения или уполномоченных по выдаче сертификатов.

"Мы считаем, что Java использовался бы шире, если бы апплетам было разрешено обращаться к жестким дискам пользователей, - говорит Патрик Тейлор, директор по маркетингу продуктов компании Internet Security Systems (ISS), производителя программных пакетов, выполняющих сканирование и проверку защиты интрасети. - Компаниям придется выработать политику, определяющую, какие из подписей в апплетах будут приниматься. При реализации защиты администраторы сети смогут останавливать подозрительные апплеты Java на брандмауэре прежде, чем они проникнут в браузер".

Важно отметить, что подписанный, сертифицированный апплет Java или управляющий элемент ActiveХ может оказаться не более доброкачественным, чем не имеющий верительных грамот. Цифровые сертификаты используют технологию шифрования для подтверждения того, что апплет или другие части кода выпущены указанным источником и переданы неповрежденными и неизмененными. Другими словами, сертификаты подтверждают подлинность апплетов, а не благие намерения его создателей. Помните, что зарегистрированное оружие может убить столь же легко, как и тайно припасенное для разбоя.

## Веб-сервер.

Web-серверы, расположенные за брандмауэром, тоже являются привлекательной целью. Захватчики могут использовать уязвимость прикладного ПО Web-серверов и операционной среды для исполнения потенциально вредных команд, получить доступ к конфиденциальным корпоративным базам данных и документам, а также к другим, связанным интрасетью компьютерам, замаскировавшись под авторизованных пользователей.

Чтобы отразить атаки на серверы, вам придется выискивать изъяны в защите приложений и операционных систем, работающих на этих машинах. "Серверы интрасети с критически важной информацией необходимо регулярно тестировать на различных уровнях, - считает Нельсон из ESTec. - После проведенных мною расследований нарушений стало ясно, что в большинстве компаний защите уровня приложения уделяется слишком мало внимания. Тестирование необходимо для оценки интерфейса между клиентом HTML и промежуточным ПО, таким как реляционные базы данных и сценарии Common Gateway Interface, а также интерфейса между промежуточным ПО и операционной системой".

Сценарии СGI, выполняющиеся на Web-сервере, являются важным связующим звеном между загружаемыми пользователем страницами HTML, базами данных, документами и другими ресурсами корпоративной интрасети. Сценарии CGI могут вызывать нарушения защиты, например заражать вирусами, обращаться к критически важным базам данных, загружая хост-компьютеры чрезмерным трафиком, и передавать файлы с паролями и информацию о системной конфигурации удаленным посторонним объектам, не имеющим соответствующих полномочий.

Эксперты по защите советуют Web-администраторам размещать все сценарии CGI в отдельном подкаталоге, открытом только для чтения, удалить все файлы с неиспользуемыми сценариями и проверить сценарии на наличие в них команд, вызывающих уязвимые исполняемые модули, такие как finger, phf, test-CGI, sh, csh, Perl, Bash и Rlogin. Однако многие сомнительные сценарии CGI были созданы на Web-серверах, разбросанных по всему миру, и администраторам Web могут быть неизвестны их уязвимые места или программные "заплатки", которые распространялись для ликвидации этих изъянов.

Рассмотрим, к примеру, сценарий phf - программу обслуживания каталога типа "белых страниц", которая была опубликована на Web-сервере Национального центра приложений для суперкомпьютеров (National Center for Supercomputing Applications, NCSA). Сценарий phf дает возможность пользователям Internet передавать символы начала новой строки в Unix-оболочку сервера Web. Это позволяет не имеющим соответствующих полномочий сотрудникам запускать любые команды на сервере и получать доступ к файлам с паролями и другой критически важной информации. Изъян обнаружен в марте 1996 г. и устранен в последующих версиях ПО, подготовленных NCSA. Но, как отмечает Хаммонд из NJH Security, "вы по-прежнему найдете людей, пытающихся получить доступ к CGI-сценарию phf, поскольку хакеры знают, что многие компании никогда не исправляют найденные ошибки".

У сетевых администраторов может возникнуть немало трудностей в связи с необходимостью поддерживать в своих сетях различные модули, которые требуется постоянно "латать", что гарантирует появление все новых и новых возможностей для старательных хакеров. ISS предлагает для решения этой проблемы программные инструментальные средства, которые автоматически сканируют серверы интрасети для поиска потенциальных недостатков защиты. Затем ПО генерирует для сетевых администраторов отчеты о защите в формате HTML.

Многие консультанты по вопросам защиты советуют радикально упростить конфигурацию серверов общего назначения, предназначенных для приложений интрасети, устанавливая только одно базовое Internet-приложение на сервер и удалив все службы, драйверы, привилегии и файлы, которые не являются абсолютно необходимыми для этой конкретной службы.

"Если у вас есть хост, который используется только для работы в Web, вы способны сконфигурировать эту систему для решения задач, касающихся исключительно Web, - подчеркивает Джонсон из SystemExperts. - С хостом, который применяется для обслуживания электронной почты, можно сделать то же самое. Однако если вы разместите службы для работы с электронной почтой и Web на одном и том же хосте, то (поскольку к ним предъявляются различные требования) набор административных возможностей и параметров, соответствующих требованиям сразу обеих служб, окажется весьма ограниченным. Это почти всегда приводит к снижению уровня защиты. Чем больше вы упорствуете, устанавливая на одном хосте Web, электронную почту, новости, маршрутизацию и так далее, тем сильнее страдает защита. Отследить причины и последствия ошибки становится практически невозможно, - утверждает Джонсон. - Пусть, скажем, риску подверглась служба электронной почты. Что делать? Вам придется отключить и все другие службы".

## Шлюзы.

Для защиты многих серверов интрасети необходимо организовать некоторую комбинацию фильтрующих маршрутизаторов, брандмауэров, proxy-серверов и модемов для доступа по телефонным линиям, которые все вместе формируют "шлюз" в вашу корпоративную сеть. Вы можете использовать эти устройства шлюзовой защиты на своем предприятии и в тех случаях, когда некоторые подразделения компании требуют оградить их информацию от других подразделений или торговых партнеров, связанных с компанией через экстрасеть, для которой открыты определенные сегменты вашей корпоративной интрасети.

Многие администраторы предпочитают устанавливать фильтрующие маршрутизаторы перед брандмауэрами уровня приложения и proxy-серверами, чтобы воспользоваться дополнительными возможностями этих технологий. "Мы серьезно анализировали вопрос об установке аппаратных маршрутизаторов защиты перед нашими брандмауэрами прикладного уровня компании Check Point Software", - говорит Харт из Университета восточного Кентукки. Он считает основными преимуществами фильтрующих маршрутизаторов (перед брандмауэрами прикладного уровня) производительность, надежность и простоту установки и администрирования. "С помощью аппаратных маршрутизаторов вы устанавливаете устройство, включаете его и оно начинает действовать. Программные брандмауэры, которые функционируют в операционных системах общего назначения, таких как Unix и Windows NT, предусматривают больше возможностей конфигурации. Следовательно, большее число сотрудников может внести ошибку". Тем не менее Харт утверждает, что "по-прежнему рассчитывает на брандмауэры прикладного уровня для выполнения более сложной проверки надежности и контроля".

Вне зависимости от того, насколько совершенны ваши брандмауэры, они не выполнят своей задачи, если управление доступом будет не очень хорошо продумано. Существуют различные подходы к выработке политики защиты при помощи брандмауэров. Некоторые эксперты считают, что паранойя - лучшая политика, и советуют администраторам интрасетей блокировать доступ из Internet к любой службе или серверу, для которых заранее точно не установлены условия открытого доступа в соответствии с бизнес-политикой компании. Другие, учитывая открытый характер среды Internet, утверждают, что надо блокировать удаленный доступ лишь к критически важным серверам баз данных интрасети или даже - исключительно при явном нарушении защиты.

Одна из традиционных проблем - недостаточная интеграция брандмауэров с другими сетевыми и компьютерными системами защиты. Ведущие производители брандмауэров решают этот вопрос, устанавливая открытые оболочки управления, в состав которых входят API и языки создания сценариев, которые предназначены для усиления интеграции с инструментальными средствами независимых производителей.

Open Platform for Security Enterprise Connectivity компании Check Point Software и Enterprise Security Architecture компании Cisco позволяют обеспечить централизованное управление защитой с консоли управления. Обе компании привлекли на свою сторону немало производителей систем защиты, в том числе поставщиков фильтрующих маршрутизаторов, систем аутентификации, наделения полномочиями, шифрования, обнаружения вторжения, проверки наличия вирусов, анализа событий и генерации отчетов. Если указанные оболочки защиты интрасети будут широко использоваться производителями систем защиты, они смогут обеспечить реакцию в режиме реального времени при нарушении защиты интрасети (к примеру, при попытке не имеющих полномочий пользователей получить доступ к критически важным Web-серверам) на любом из корпоративных брандмауэров. Затем брандмауэр будет динамически изменять управление доступом, чтобы не пропустить нарушителя. Брандмауэр также мог бы динамически вызывать соответствующие средства защиты, такие как аплеты Java и модули, определяющие наличие вируса, для разрешения этой проблемы. Другими словами, фильтрация и правила, используемые для проверки надежности защиты периметра интрасети, могли бы изменяться в реальном времени - в зависимости от событий, происходящих в интрасети. Алекс Хенторн, менеджер по системам защиты компании Livingston Enterprises, производящей брандмауэры на основе маршрутизаторов, утверждает: "Брандмауэры предназначены для того, чтобы сбить темп атаки и принять соответствующие меры".

# Заключение

В рамках данной лабораторной работы была освоена терминология, связанная с санкционированием доступа к информации, были описаны основные уязвимые места в звеньях интерсети и способы повышения безопасности. Вывод можно сделать следующий: защита интрасети невозможна без дисциплины. Информированность администраторов сети о последних угрозах "нападения" строго обязательна. Хорошо продуманный план защиты вселит в вас уверенность и даст возможность быстро отреагировать при возникновении непредвиденных ситуаций.