5 Підготовка, перепідготовка та підвищення кваліфікації спеціалістів систем захисту інформації

УДК 681.3.06

ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ДИСТАНЦИОННОМ ОБРАЗОВАНИИ

Айдын Гасанов

Национальная Академия наук Украины и Министерство науки и образования Украины, Международный научно-учебный центр информационных технологий и систем

Аннотация: **На основе обзора литературных источников изложены некоторые технические предложения по защите информации в дистанционном образовании.**

Summary: **Some technical measures for information defense in distance learning systems have been proposed in this report on base of analyzing of reference from literature.**

Ключевые слова: **Защита информации, удаленный пользователь, каналы связи.**

I Образовательные услуги в системе дистанционного обучения

Современная компьютерная практика характеризуется непрерывным появлением новых технологий. С использованием новых коммуникативных технологий стало возможным расширить область применения персональных компьютеров, особенно в глобальной компьютерной сети Интернет. При этом в распоряжение пользователя поступает новейшая информация о текущих событиях и современной технике, а также возможность получения квалифицированного совета практически по всем проблемам современной жизни.

Большая часть информации научной, образовательной, специальной, в передовых технологиях, какими являются WWW-технологии, могут носить конфиденциальный характер, а следовательно возникают вопросы защиты и безопасности информации, представленной в Интернет.

Развитие средств информатизации и дистанционного общения за последние десятилетия существенно расширило сферу их проникновения в различные стороны педагогической деятельности: от создания отдельных электронных учебников до конструирования сложных виртуальных сред общения в процессе обучения. При этом увеличивается аудитория обучаемых, требующих различную степень конфиденциальности необходимой им учебной информации. Использование учебных курсов в системе дистанционного обучения производится через программную среду, обеспечивающую выполнение целого набора функций, основными из которых являются: защита от несанкционированного доступа; авторизация доступа; структуризация пользователей по категориям и наделение каждой категории определенными полномочиями; формирование каталога информационных ресурсов, находящихся в данной программной среде и др. [1].

Образовательные услуги в системе дистанционного обучения могут быть основаны на разной модели обучения. Целесообразно выделить пять моделей организации образовательного процесса [2]. За основание классификации моделей принято средство доставки учебных материалов и требуемый уровень защищенности информации (табл. 1).

Отличие моделей друг от друга заключается в следующем.

Кейс-технология характеризуется обязательным посещением учебного центра. Контролируемая самостоятельная работа составляет основу учебного процесса.

В корреспондентском обучении информационный обмен осуществляется через традиционную почту. Модель в целом ориентирована на случаи, когда в месте обучения студента отсутствует телекоммуникации. В основе данной модели лежит интерактивный процесс постоянного обмена по почте или каким-то другим способом между преподавателем и студентом учебными материалами, домашними заданиями и результатами.

В радиотелевизионной модели для доставки к обучающемуся учебной информации могут использоваться телевидение, радио, радиотрансляционные городские сети. Для доставки материалов, представленных в электронном варианте, возможно также использование и других систем.

Модель сетевого обучения базируется на использовании сети Интернет. При этом оформляются и отправляются в центр необходимые документы, представленные в электронном виде. После прохождения

формальных процедур по оформлению и оплате курса, обучающийся получает пароль для санкционированного доступа к учебной информации и фамилию преподавателя для индивидуальных консультаций и сдачи промежуточных тестов. Взаимосвязь студента с преподавателем организуется по электронной почте, теле- или видеоконференцсвязи или их комбинации.

Таблица 1 – Средство доставки учебных материалов и требуемый уровень защищенности

Модели обучения	Предоставленный учебный материал	Средства дидактического взаимодействия	Уровень защищенности
Кейс технология	Учебные пособия. Программы на CD-ROM или другом носителе	Телефон Факс	Низкий
Корреспондентская	Учебные пособия. Программы на CD-ROM или другом носителе	Обычная (традиционная почта).	Низкий
Радиотелевизионная	Обучающие программы в электронном виде (цифровой аналог).	Электронная почта. Телеконференция	Средний
Сетевая	Гипертекст Гипермедиа	Электронная почта. Телеконференция	Высокий
Мобильная	Электронная форма	Электронная почта. Телеконференция	Наивысший

В последней рассматриваемой модели обучения студент использует **мобильный** персональный портативный компьютер, в память которого могут быть записаны электронные курсы для последовательного во времени изучения учебного материала. По мере изучения учебный материал обновляется путем перезаписи с настольных персональных компьютеров учебных центров в мобильный персональный компьютер через инфракрасную или кабельную связь. Наиболее сложные и дорогие из этих компьютеров являются полнофункциональными с выходом в Интернет. В этом случае модель проведения учебного процесса не отличается от сетевого метода обучения.

II Способы обеспечения безопасности в различных сферах

Связь пользователя с электронной информацией может быть доступной, защищенной ключом, паролем и криптографическими методами. Могут быть использованы также возможности опосредованного наблюдения за характером работы пользователя. Рассмотрим возможные способы обеспечения безопасности информации с учетом различных пользователей, представленные на рис. 1.

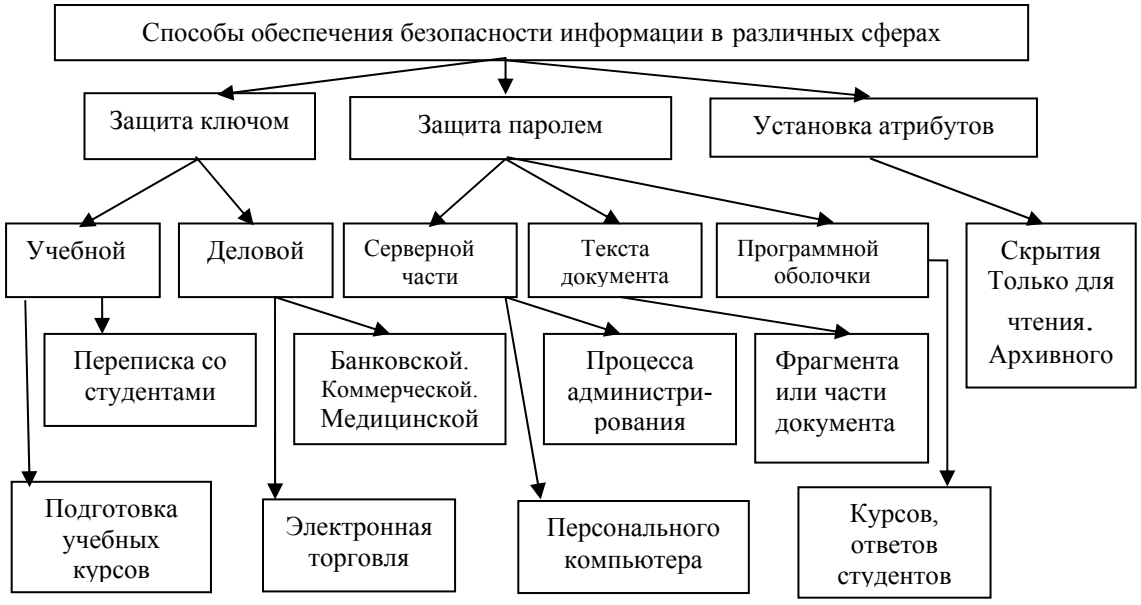

Рисунок 1 – Способы обеспечения безопасности информации

Защита ключом. Чтобы зашифровать и расшифровать сообщение пользователю потребуется ключ. Обычная процедура шифрования требует наличия у отправителя и у адресата одинакового ключа, однако нельзя допустить, чтобы ключ мог попасть к чужому пользователю. Безопасные методы управления ключами имеют важное значение. Все системы используют в этом случае два ключа – открытый и секретный, являющиеся буквенно-цифровыми строками. Открытый ключ сообщается всем, и каждый пользователь может использовать его для того, чтобы послать зашифрованное сообщение. Секретный ключ сохраняется в зашифрованном файле и защищен паролем с использованием сертификатов [3]. Сертификат открытых ключей – это структура данных, содержащая имя пользователя, открытый компонент (модуль, задействованный в расчетах алгоритма RSA, названного в честь его создателей Rivest, Shamir, Adelman) этого пользователя и имя издателя, которое гарантирует, что данный доступный компонент соответствует данному пользователю. При этом широко используется симметричная криптосистема, в котором отправитель и получатель имеют общий ключ обмена. В отличие от симметричных, в ассимметричных криптосистемах открытым является только ключ получателя. В простейшем виде сертификатом является цифровой документ, который связывает открытый ключ с определенным пользователем. Простейший способ хранения секретных ключей – это зашифровать их паролем и записать на диск (например, флоппи-диск). Благодаря криптографическому алгоритму несимметричного RSA-преобразования, стало возможным разделение применяемых ключей на открытые и конфиденциальные (личные).

Защита паролем. При входе пользователя в систему программа login проверяет, зарегистрирован ли пользователь в системе и знает ли он правильный пароль, образует новый процесс и запускает требуемую для данного пользователя программу доступа, после реализации которого для этого процесса начинают действовать ограничения на доступы к файлам.

Установка атрибутов. Атрибуты определяют некоторые системные свойства файлов и каталогов. Они могут быть назначены администратором для любого сетевого файла или каталога. Например, чтобы записать данные в файл, пользователь должен знать собственный идентификатор и пароль для подключения к сети, иметь право записи данных в файл (файл должен иметь атрибут, разрешающий запись данных). Следует отметить, что атрибуты файла и каталога имеют более высокий приоритет, чем права пользователей по отношению к этому файлу.

Защита информации при обучении студентов гражданских учебных заведений отличается от защиты информации при обучении курсантов военных училищ. Разнообразные курсы, даже гражданских вузов, также могут требовать различную степень защищенности информации.

Рассмотрим группы пользователей и требования к защищенности информации. На рис. 2 приведены возможные уровни защищенности, присвоенные тем или иным пользователям [4].

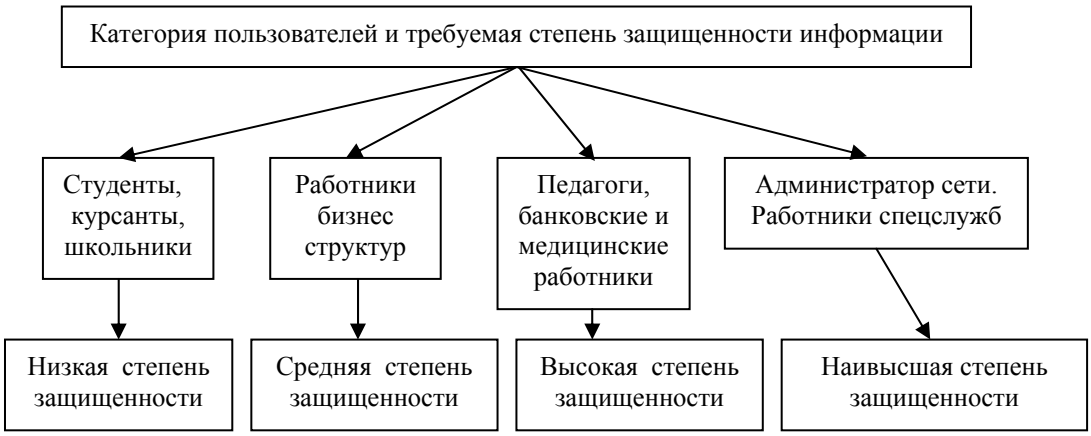

Рисунок 2 – Степень защищенности информации для различных категорий пользователей

Имеются несколько уровней защиты: **низкая, средняя, высокая и наивысшая**.

Низкая степень защиты характеризуется наличием подсистемы учета событий, связанных с безопасностью и избирательным контролем доступа.

Средняя степень защиты характеризуется присутствием средства секретного входа, обеспечивающего идентификацию пользователей путем ввода уникального имени и пароля перед тем, как им будет разрешен доступ к системе. Избирательный контроль, требуемый на этом уровне, позволяет владельцу ресурса определить, кто имеет доступ к ресурсу и что он может делать с ним.

Высокая степень защиты с помощью средств учета и наблюдения (auditing) дополнительно к первым трем степеням защиты, обеспечивает возможность обнаружить и зафиксировать важные события, связанные с безопасностью или удалением системных ресурсов.

Наивысший уровень защиты – самый высокий уровень безопасности – реализует мандатный контроль доступа. Каждому пользователю присваивается рейтинг защиты и он может получать доступ к данным только в соответствии с этим рейтингом. На этом уровне также возможно выполнение формального, математически обоснованного доказательства соответствия системы требованиям безопасности.

Согласно описанным степеням защиты при трехуровневой системе защиты данных архитектуру взаимосвязи доступа к данным, файлам и каталогам можно представить в виде, изображенном на рис. 3.

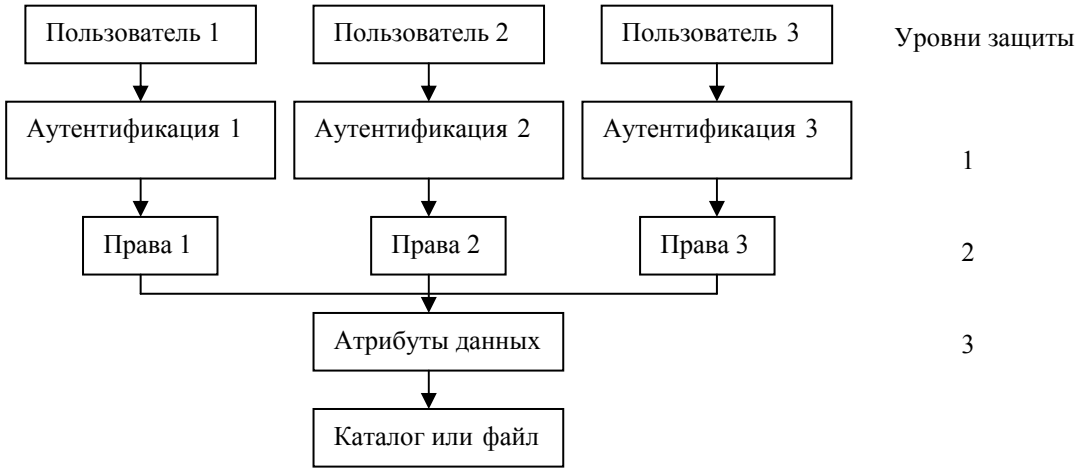

Рисунок 3 – Архитектура доступа к файлам и каталогам при трехуровневой системе защиты

Права по отношению к файлу или каталогу определяют, какие операции пользователь может выполнить с файлом или каталогом. Администратор сети может для каждого пользователя сети определить его права по отношению к любому сетевому файлу или каталогу.

Все ресурсы программного обеспечения (ПО) в дистанционном обучении разделены на две части: открытую и закрытую. Открытая часть ПО доступна любому пользователю Интернет и содержит следующие основные разделы: правила приема с указанием специальностей, уровней подготовки и учебных планов по каждой специальности; список учебных курсов и стоимость обучения по каждому из них; демонстрационную версию одного курса; интерактивную страничку обратной связи; правила регистрации; типовой договор для проведения регистрации в режиме on-line.

Закрытая часть доступна только зарегистрированным пользователям данной системы. Для каждой категории пользователей определен и доступен только фиксированный набор функций. Регистрацию новых пользователей обычно выполняет администратор системы. Пароли хранятся в отдельном файле в закодированном или зашифрованном виде. При входе в систему пользователь получает неограниченный доступ к своему каталогу и файлам, содержащимся в нем. Возможен доступ ко всем другим файлам, однако он может быть ограничен, если пользователь не имеет достаточных привилегий.

III Способы подключения удаленных пользователей к глобальным сетям

Особенностью дистанционного обучения является то, что обучаемые могут находиться далеко от обучающих их преподавателей. Для интерактивного взаимодействия преподавателей со студентами могут использоваться как Интернет, так и телефонные линии связи. Большую опасность представляют соединения пользователей через Интернет.

Существуют различные способы подключения удаленных пользователей к Интернет. Услуги по подключению к сети Интернет предоставляются сервис-провайдерами, имеющими компьютерную сеть, которая постоянно соединена с Интернет. Основные методы доступа в Интернет представлены на рис. 4 [5].

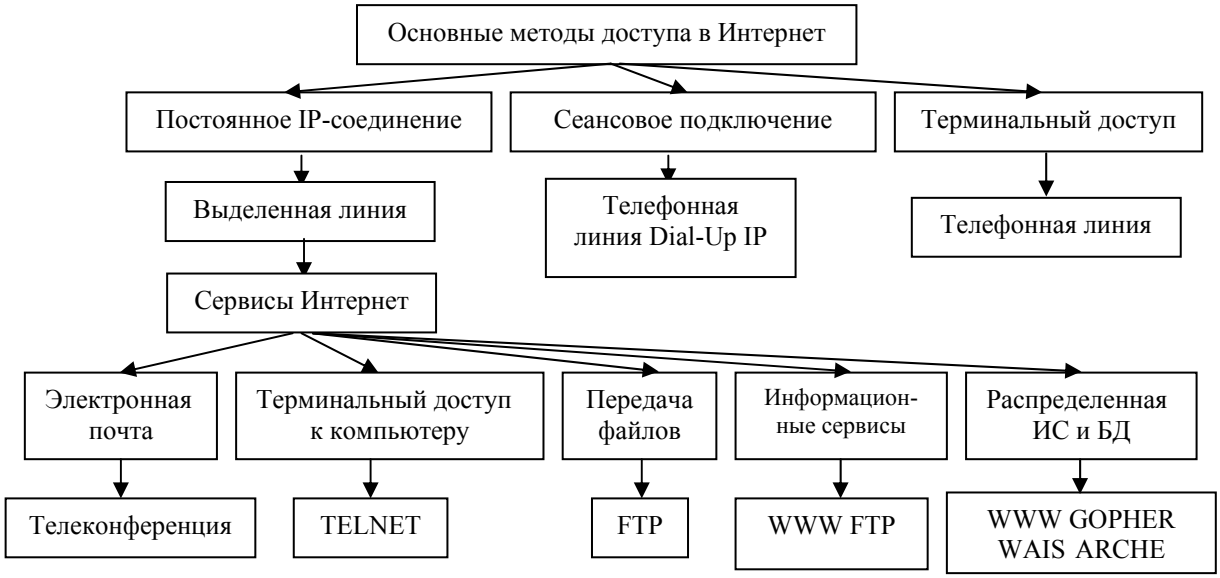

Рисунок 4 – Основные методы доступа в Интернет

1. Особенностью постоянного Internet Protocol (IP) соединения через выделенную линию является работа в локальной сети, подключенной к Интернет по выделенной линии. В этом случае один из компьютеров локальной сети, называемый маршрутизатором, имеет постоянное соединение с маршрутизатором поставщика и обеспечивает передачу пакетов для рабочих станций локальной сети (IP-соединение по коммутируемой линии применяется в основном для подключения одиночных персональных компьютеров к Интернету).

На рис. 5 представлена схема передачи IP-пакетов по выделенной линии.

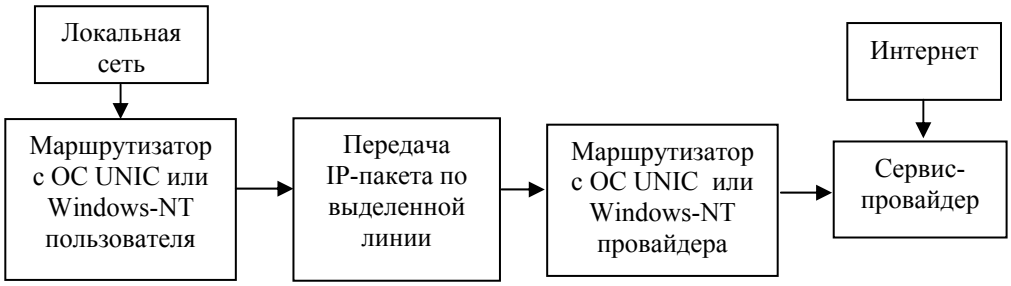

Рисунок 5 – Передача IP – пакета по выделенной линии

2. В методе сеансового подключения по коммутируемой линии (Dial-Up IP) копьютер пользователя будет подключен к Интернет на протяжении сеанса телефонной связи. Сеанс IP-подключения позволяет получать доступ ко всем ресурсам Интернет путем запуска на компьютере пользователя соответствующих прикладных программ.

3. В методе терминального доступа к удаленному компьютеру (on-line-технология) соединение осуществляется по телефонной линии и не требует высокого качества телефонной линии, характеристик компьютера и модема абонента. При этом передается только текстовая информация. Основным ограничением режима удаленного терминала является то, что пользователь фактически работает не на своем, а на хост-компьютере провайдера. Предоставляемый сервис – электронная почта, TELNET, File Transfer protocol (FTP), работа с универсальным Web-клиентом (например lynx).

4. Услуги электронной почты (off-line технология) предлагаются многими поставщиками и могут предоставляться как частному лицу для получения почты на домашний компьютер, так и фирме, в которой можно организовать работу с почтой всех или некоторых пользователей локальной сети. При помощи электронной почты можно посылать не только текстовые сообщения, но и двоичные файлы (отформатированные документы текстовых и табличных процессоров, файлы с графическими изображениями, исполняемые программы).

IV Характеристика угроз безопасности информации при удаленном доступе

Разнообразие методов доступа удаленных пользователей приводит к уязвимости информации и требует разнообразных методов ее защиты. Некоторые из методов доступа описываются далее.

Удаленный доступ по телефонному каналу: уязвим с помощью «боевых дилеров» – простых программ, использующих модемы с автодозвоном для сканирования блоков телефонных номеров и выявления номеров с модемами; часто злоумышленники представляются сотрудниками отделов технической поддержки для того, чтобы узнать у законных пользователей их пароли;

TELNET обычно требует отправку информации, предназначенной для входа пользователя в систему, имени и пароля по телефонному каналу в незашифрованном виде, уязвимом с точки зрения безопасности.

Удаленный доступ с помощью переносного компьютера. При использовани компьютера в аэропорту, в самолете возможно подглядывание злоумышленников из-за плеча, в результате чего могут быть раскрыты данные и пароли. При нахождении без присмотра данные, хранимые на диске, уязвимы к копированию или неавторизованному чтению. При утере переносного компьютера служащие не сразу сообщают о пропаже, что делает вполне возможным удаленный доступ злоумышленника.

Электронная почта. Основными протоколами в Интернете (не считая частных протоколов, шлюзуемых, или туннелируемых через Интернет) являются Simple Mail Transport Protocol (SMTP), Post Ofis Protocol (POP), Internet Mail Acces Protocol (IMAP). Использование электронной почты (e-mail) для осуществления важных деловых взаимодействий растет быстрыми темпами. Этот вид связи имеет следующие виды угроз: адреса e-mail в Интернете легко подделать; электронные письма могут быть легко модифицированы, так как стандартное SMTP–письмо не содержит средств проверки целостности передаваемой информации; текст письма может быть прочитан на каждой промежуточной станции; обычно нет гарантий доставки e-mail.

V Угроза безопасности сервисам Интернет

Соединение с Интернет делает доступными для внутренних пользователей разнообразные сервисы, а для внешних пользователей – доступ к большому количеству персональных компьютеров.

Ниже приведены сервисы Интернет, представляющие угрозу безопасности [6].

- R-команды BSD Unix, такие как rsh, rlogin, rcp и другие, предназначенные для выполнения команд пользователя Unix-систем на удаленных системах. Большинство их реализаций не поддерживают аутентификации или шифрования и являются очень опасными при их использовании через Интернет.
- Протокол почтового отделения POP является протоколом клиент-сервер для получения электронной почты с сервера. POP использует Transmission Control Protocol (TCP) и поддерживает одноразовые пароли для аутентификации. POP не поддерживает шифрования, доступные для чтения письма. Они могут быть перехвачены.
- Протокол чтения сетевых новостей NNTP использует TCP и является протоколом с многоэтапной передачей информации, который также представляет угрозу безопасности.
- Finger и whois выполняют похожие функции. Finger используется для получения информации о пользователях системы. Finger и whois уязвимы, должны быть отключены с помощью брандмауэра.
- Сетевая файловая система Network file system (NFS) позволяет создавать дисковые накопители, доступные для пользователей и систем в сети. NFS использует слабую форму аутентификации и считается небезопасным при использовании его в недоверенных сетях. NFS должен быть запрещен с помощью брандмауэра.
- Живое аудио (real audio) позволяет получать оцифрованный звук по сетям TCP/IP. Кроме него был разработан еще ряд сервисов для использования мультимедийных возможностей WWW. Считается небезопасным, так как непосредственная связь пользователей осуществляется через Интернет.
- Веб-страницы часто включают конфиденциальную информацию. Как и e-mail, данные, посылаемые веб-броузером на веб-сервер, проходят через большое число промежуточных компьютеров и сетей до того, как достигнут своего конечного назначения. Любая важная информация, посылаемая с помощью ввода данных на веб-странице, может быть перехвачена.
- SMTP – это почтовый протокол хост-хост. SMTP-сервер принимает письма от других систем и сохраняет их в почтовых ящиках пользователей. Сохраненные письма могут быть прочитаны несколькими способами. Пользователи могут загрузить свои письма с помощью программ – почтовых клиентов по протоколам POP3 и IMAP. Широко используемый SMTP-сервер является Sendmail. Если его не защитить, то атакующий сможет нанести вред электронным письмам.
- IMAP-протокол чтения e-mail, уязвим.

- MIME – для многоцелевых расширений Интернетовской почты. Он переопределяет формат сообщений e-mail и позволяет организовать: передачу текстов в кодировке, отличной от US-ASCII; передачу в письме нетекстовой информации в различных форматах; передачу сообщения, состоящего из нескольких частей. Поддерживает такие средства безопасности, как цифровые подписи и шифрованные сообщения. Обеспечивает взаимодействие при гарантии безопасности электронной почты.

VI Способы защиты электронной почты

Имеются угрозы, связанные с электронной почтой, так как основные протоколы передачи почты (SMTP, POP3, IMAP4) обычно не осуществляют надежной аутентификации. Это позволяет легко создать письма с фальшивыми адресами. Ни один из описанных протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем.

На рис. 6 приведены различные способы защиты электронной почты.

Рисунок 6 – Способы защиты электронной почты

Защита от фальшивых адресов. От этого можно защититься присоединением к письмам электронных подписей с помощью шифрования. Одним из популярных методов является шифрование с открытым ключом. Однонаправленная хэш-функция письма шифруется, используя секретный ключ пользователя. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией после получения сообщения. Это гарантирует, что сообщение на самом деле написано отправителем, и не изменено в пути.

Защита от перехвата. От перехвата можно защититься с помощью шифрования содержимого сообщения или канала, по которому передается сообщение. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Из предложенных схем шифрования самая популярная – PGP, использующая лицензированную версию алгоритма шифрования с открытым ключом RCA.

Защита брандмауэром. Брандмауэр является техническим средством защиты, которое используется для управления доступом к глобальным сетям между надежной и менее надежной сетями. Основная его функция заключается в централизации управления доступом. На рис. 7 представлены различные типы брандмауэров.

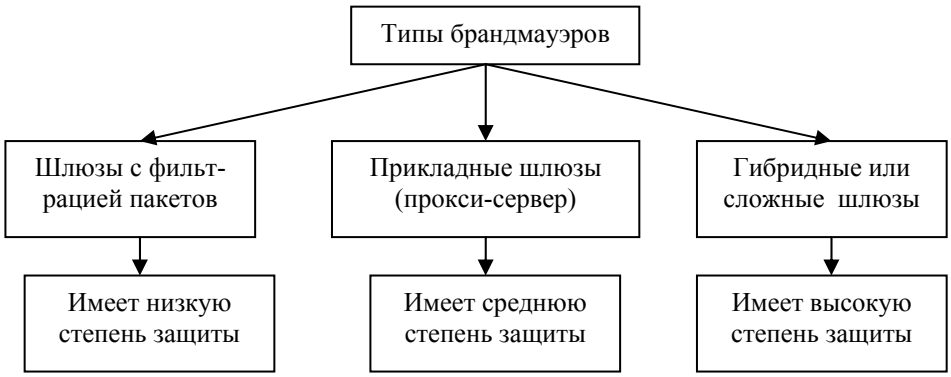

Рисунок 7 – Типы брандмауэров

Брандмауэры с фильтрацией пакетов используют маршрутизаторы с правилами фильтрации пакетов для предоставления или запрещения доступа на основе адреса отправителя, адреса получателя и порта. Недостатки этой защиты заключаются в следующем: адреса, порты отправителя и получателя, содержащиеся в заголовке IP-пакета, – единственная информация для принятия решения о запрещении или разрешении

доступа трафика в сеть, доступная маршрутизатору. Такие пакеты не защищают от фальсификации IP- и DNS-адресов и не поддерживают аутентификации пользователя.

Прикладные шлюзы используют программы (иначе называются прокси-серверы), запускаемые на брандмауэре, которые принимают запросы извне, анализируют их и передают безопасные запросы внутренним хостам, которые представляют соответствующие сервисы. Прикладные шлюзы могут обеспечивать такие функции, как аутентификация пользователей и протоколирование их действий.

Различные схемы использования брандмауэра в удаленном доступе представлены на рис. 8 и 9.

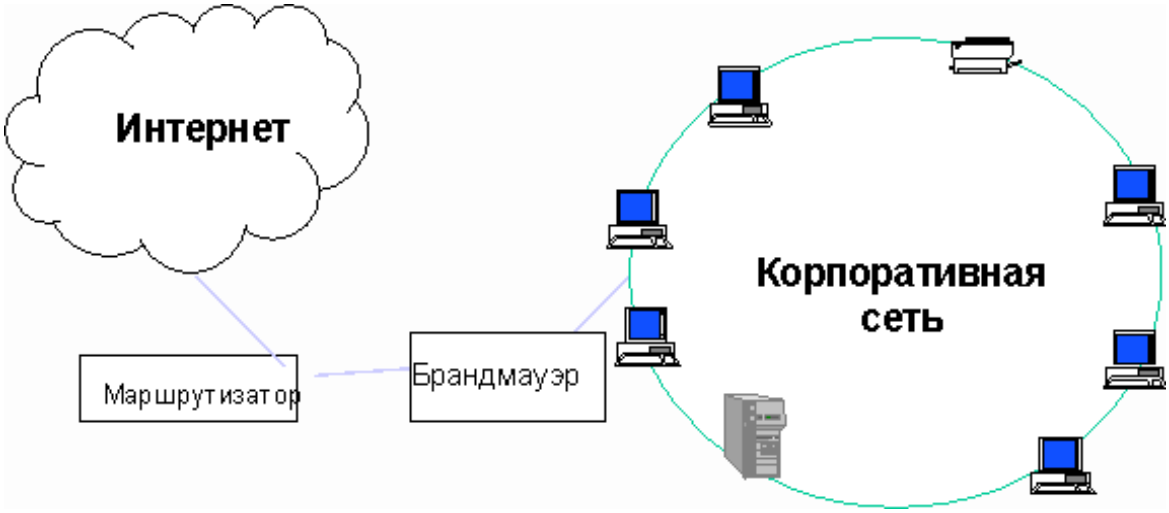

Рисунок 8 – Схема использования брандмауэра в удаленном доступе

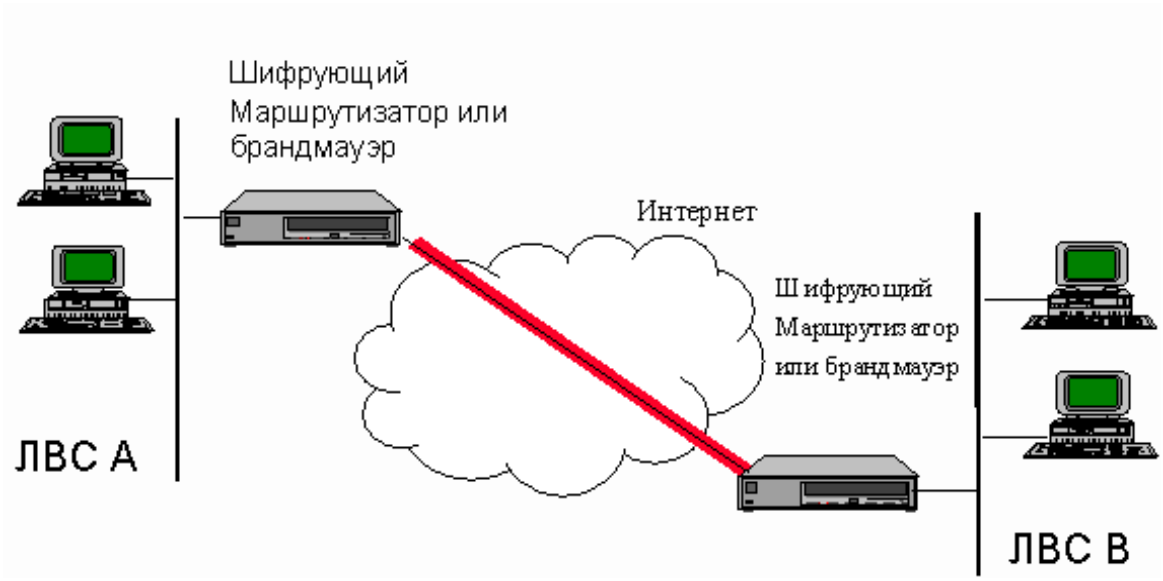

Рисунок 9 – Конфигурация удаленного доступа по коммутируемым каналам с использованием двух брандмауэров

VII Заключение

На основании приведенной классификации доступа к глобальной сети определен требуемый уровень защищенности информации для различных групп удаленных пользователей.

Используя механизмы авторизации доступа к данным сети при трехуровневой защите можно предотвратить доступ злоумышленников. В этом случае при аутентификации подтверждается не только

подлинность пользователя при его подключении к сети, но и подлинность пакетов, передаваемых между сервером и рабочей станцией.

Большую опасность представляют соединения пользователей по Интернет. Разнообразие методов доступа удаленных пользователей приводит к уязвимости информации и требует разнообразных методов защиты – таких как защита от фальшивых адресов, защита от перехвата, защита брандмауэром.

Литература: 1. Тихомиров В. П., Солдаткин В. И., Лобачев С. Л., Ковальчук О. Г. Дистанционное обучение: к виртуальным средам знаний (часть 1). – Дистанционное образование. – 1999. № 2. – С 8-15. 2. Андреев А. А., Солдаткин В. И. Дистанционное обучение: сущность. технология. – М: издательство МЭСИ. – 1999. – 196 с. 3. Бабушкин М., Иваненко С., Коростелев В. Веб-сервер в действии – СПб: Питер. – 1997. – 416 с. 4. Gasanov A. S., Melnyk I. V. Problems of defence and security of information in distance learning systems / Telematics and Life-Long Learning. Proceedings of the International Workshop. TLLL-2001. October 15-17, 2001, Kyiv, Ukraine. – P. 57. 5. Кухаренко В. М., Кудрявцева С. П., Колос В. В., Монако А. Ф., Цыбенко Ю. В. Основы Интернет. Дистанционный курс. – Харьков: ХДПУ – 1998. – 88 с. 6. Вакка Дж. Секреты безопасности в Internet. – К.: Диалектика. – 1997. – 512 с.

УДК 621.396

ДОСВІД ПІДГОТОВКИ ФАХІВЦІВ З ПИТАНЬ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Володимир Голубєв

Центр Дослідження Проблем Комп'ютерної Злочинності

Анотація: **Розглянуто досвід впровадження дисципліни "Методика розслідування комп'ютерних злочинів" та підготовки фахівців-правоохоронців з питань попередження та розслідування комп'ютерних злочинів у Гуманітарному університеті "Запорізький інститут державного та муніципального управління".**

Summary: **Experience of introduction of discipline " The procedure of investigation of computer crimes " and preparations law enforcement on questions of the prevention and investigation of computer crimes at Humanitarian University " Zaporozhye Institute of the State and Municipal Management ".**

Ключові слова: **Навчання, методика розслідування, комп'ютерні злочини.**

I Вступ

Подібно багатьом революційним технологіям – комп'ютерні технології несуть з собою величезний потенціал як для прогресу так і для зловживань. Атаки у мережі, шахрайство, програмне піратство, технічне шпигунство, торгівля дитячою порнографією – тільки деякі зі злочинів, що вчиняються сьогодні у глобальній інформаційній мережі Internet.

Зростання науково-технічної озброєності злочинних угруповань об'єктивно впливає на використання правоохоронними органами сучасних інформаційних технологій, а також нових негласних засобів оперативно-розшукової діяльності (ОРД) у боротьбі зі злочинністю. Наприклад, жорсткі диски персональних комп'ютерів торговців наркотиками та зброєю можуть містити фінансові записи та дані щодо поставок та клієнтів. У випадку використання інформаційних технологій для планування або вчинення злочину з комп'ютера злочинця можна вилучити план вчинення пограбування або вбивства.

Для законного зняття комп'ютерної інформації потрібні спеціальні технічні засоби, у тому числі чітка юридична основа для установки таких засобів, але все це неможливо без спеціальної підготовки органів дізнання, суб'єктів ОРД.

Особливі труднощі викликають первісні слідчі дії, зв'язані з розслідуванням транснаціональних комп'ютерних злочинів (кіберзлочинів), що пов'язано з багатьма проблемами [1].

Результати досліджень, що проводяться Центром Дослідження Проблем Комп'ютерної Злочинності, та аналіз практичної діяльності правоохоронних органів щодо розслідування комп'ютерних злочинів свідчать, що дослідження комп'ютерної техніки, яка вилучається на місці події, доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою.

Інше питання, де сьогодні взяти таких фахівців, коли не один з ВУЗів України їх ще не готує. Отже, сьогодні назріла гостра потреба у підготовці та перепідготовці співробітників правоохоронних органів, які спеціалізуються у боротьбі з комп'ютерною злочинністю.