реальными экспериментальными установками и объектами. Функции учителя на этом этапе сводятся к консультированию учеников.

Третий этап представляет собой выполнение эксперимента в реальных условиях. Для этого может быть использован режим удаленного доступа к экспериментальной установке. На этом этапе основная педагогическая нагрузка ложится на учителя, который организует лабораторный практикум и оказывает помощь учащимся. Отчет по выполненным работам представляется для проверки учителю.

Таким образом, лабораторные и практические работы как формы учебной деятельности при дистанционном обучении предполагает усиление роли учителя по консультационному и контролирующему сопровождению учебно-познавательной деятельности учащихся, а также увеличение самостоятельной работы учащихся с учебно-методическими материалами.

Библиографический список

1. Новые педагогические и информационные технологии в системе образования: учеб. для студ. высш. учеб. заведений [Текст] / Е. С. Полат, М. Ю. Бухаркина, М. В. Моисеева, А. Е. Петров; под ред. Е. С. Полат. - 4-е изд., стер. - М.: Академия, 2009. - 272 с. - (Высшее профессиональное образование).

2. Педагогические технологии дистанционного обучения: Учеб. пособие для студ. высш. учеб. заведений / [Е. С. Полат, М. В. Моисеева, А. Е. Петров и др.]; под ред. Е. С. Полат. - 2-е изд., стер. - М.: Издательский центр "Академия", 2008. - 400 с. - (Высшее профессиональное образование.

3. *Полат Е.С, Моисеева М.В., Петров А.Е.* Педагогические технологии дистанционного обучения [Текст]: Учебное пособие для студентов вузов / Под ред. Е. С. Полат — М., "Академия", 2006. – 400 с.

4. Учимся дома: дистанционное обучение [Текст] / авт.-сост. В. Н. Пунчик [и др.]. - Минск: Красико-Принт, 2009. - 176 с. - (Педагогическая мастерская).

5. *Хуторской, А.В.* Практикум по дистанционному обучению. [Текст] /А.В. Хуторской. — М.: ИОСО РАО, 2000. – 304 с.

Е.А. Голованов, А.А. Шайдуров

СОВРЕМЕННЫЕ СПОСОБЫ ОБЩЕНИЯ. ПРОБЛЕМЫ ИХ БЕЗОПАСНОСТИ.

zdali@mail.ru

Российский государственный профессионально-педагогический университет, Екатеринбург

Для связи различных компаний из разных городов раньше использовали стационарную телефонную связь, но это не защищенный канал связи, к которому часто подключаются злоумышленники. В современном обществе существует VoIP телефония и электронные почтовые службы. В каждой области можно выделить самые популярные сервисы и соответственно выявить их проблемы.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность[1]:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Среди продуктов, работающих на базе VoIP телефонии, самая популярная программа это Skype.

Skype – бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь через Интернет между компьютерами, а также платные услуги для звонков на мобильные и стационарные телефоны.

Этот вид связи актуален и часто используется для деловых переговоров. При видео звонке можно увидеть собеседника, подобие личной встречи, но на большом расстоянии друг от друга. Используя функцию, «демонстрация экрана» можно показать презентацию или бизнес план. Телеконференция удобный способ для организации совещания по экстренным вопросам. При необходимости можно прислать, какой либо документ, т.к. Skype поддерживает обмен файлов. Skype очень удобная и многофункциональная программа, которая используется во всем мире. Установив данную программу, организация сталкивается с 2 проблемами:

- Как защитить данные;
- Как ограничить от злоумышленного использования программы.

Даже установив специальную программу для бизнеса и создав специальных учетных пользователей с отчетностью, все равно рабочий может использовать стороннюю учетную запись и передать конфиденциальные данные.

Skype активно изучается в хакерских лабораториях и security-организациях по всему миру, и большинство исследователей единодушно сходятся во мнении, что Skype - это программа, написанная талантливыми людьми Никласом Зеннстрёмом и Янусом Фриисом[2].

Ефиму Бушманову удалось воспроизвести код протокола для первой, третьей и четвертой версий клиента Skype, а также разобраться в алгоритмах шифрования, которые использует сервис. Свои наработки 3 июня 2011 он разместил на файлообменнике Depositfiles.com и на сервисе The Pirate Bay и дал ссылки на них в своем блоге. При этом разработчик уточнил, что использовал устаревшую версию протокола Skype, уже вышедшую из употребления[6].

В некоторых странах существует запрет на использование Skype, таких как Китай, Объединённые Арабские Эмираты. В России так же пытались ввести запрет, аргументируя угрозой безопасности связанной с шифрованием разговоров. В ответ на попытки запрета Skype, его разработчики начали внедрять в программу средства маскировки трафика для обхода блокировки VoIP. Кроме того, Skype может работать внутри анонимной сети I2P, подвергаясь при этом дополнительному многоуровневому шифрованию и анонимизации, также Skype может работать с прокси-серверами, VPN и Tor, что практически сводит на нет эффективность его блокировки.

Хакеры уже давно догадались использовать Skype для распространения вирусов и организации распределенных атак, которым очень сложно воспрепятствовать - Skype-трафик надежно зашифрован и не может быть проанализирован антивирусами, заблокирован брандмауэрами или распознан системами обнаружения вторжения[5].

На момент написания статьи работы по обеспечению защищенной работы Skype ведутся компанией Searchinform которая предоставляет услуги комплексной защиты на территории Украины и России. Компания разработала программу Skypesniffer, которая

предоставляет возможности мониторинга деятельности сотрудников не только путём контроля голосового канала общения, но также контроля передачи текстовых сообщений, SMS и файлов по протоколу Skype. SearchInform SkypeSniffer позволяет оперативно анализировать передаваемую по данному протоколу информацию и мгновенно предотвращать утечки[4].

Возможностями интернет-почты пользуется каждый на сетевых просторах. Самые популярные почтовые домены mail.ru, yahoo.com, rambler.ru и yandex.ru, насчитывают миллионы зарегистрированных пользователей, и каждый день эта цифра увеличивается. Почта используется как рядовыми пользователями, так и разнообразными фирмами, организациями, компаниями для связи. Как следствие появились и люди, которые заинтересовались в получении доступа к почтовому ящику для получения конфиденциальной информации и если получен доступ есть возможность удаления информации не оставив при этом следов взлома.

Поэтому они стали искать разнообразные уязвимые места в безопасности. Прошло уже много времени с момента обнаружения и устранения первых уязвимостей, но проблема защиты почтового аккаунта остается актуальной на сегодняшний день.

Чтобы защититься от несанкционированного взлома, необходимо знать методы, которыми пользуются злоумышленники при попытке получить доступ.

В первую очередь рассмотрим социальную инженерию. Социальная инженерия – очень мощное средство взлома. Метод основан на психологическом факторе, а точнее, на постоянных человеческих ошибках. В основном это обман пользователя или введение его в заблуждение. Очень часто для взлома почтового ящика злоумышленник отправляет жертве письмо от имени администрации, где сообщает о проведении смены оборудования на сервере и просит прислать логин и пароль – в ином случае электронная почта будет удалена. Запомните, никогда и ни под каким предлогом никому не следует передавать логин и пароль.

Второй способ получения доступа – вредоносные программы.

Почтовая рассылка сообщений уже многие годы является способом распространения вредоносных программ. Злоумышленники распространяют вирусы с поздравительными открытками в праздничные дни, такие как 23 февраля, 8 марта и другие праздники, когда многие рады увидеть открытку или поздравление, не подозревая о злом умысле. Противодействием в данном случае будут служить антивирус и сетевой экран. Первый не даст уже известным вредоносным программам этого типа запуститься на компьютере и выполнять свои злые намерения, а второй будет контролировать работу всех приложений с сетью и отлавливать подозрительные попытки отправки почты.

Еще один способ получения неправомерного доступа к электронной почте – Ответ на контрольный вопрос. При регистрации почты предоставляется несколько способов восстановления пароля и один из них ответ на контрольный вопрос, как правило, это стандартные вопросы предложение сервисом электронной почты. Узнать ответ на эти вопросы абсолютно несложно – достаточно познакомится с жертвой и как-нибудь узнать ее любимое блюдо или имя домашнего питомца. Узнав, взломщик получает возможность задать новый пароль для почты жертвы. Для защиты от этого способа взлома можно не использовать контрольный вопрос или не надо использовать такие банальные и стандартные вопросы. Лучше всего указать свой, причем ответ на него должны знать только вы.

Целью злоумышленников могут быть не случайные люди, получившие рассылку сообщений с рекламой или поздравлениями, а так же нацеленные атаки. Так, например, в феврале были взломаны десятки электронных почтовых ящиков, принадлежащих представителям администрации сирийского президента. В результате взлома вся переписка была размещена в открытом доступе. Одной из причин взлома специалисты называют слишком простые пароли, которые использовались помощниками и советниками президента Сирии для доступа к почте [3].

Этот способ называется взлом брутфорсом. Brute force переводится с английского как «грубая сила». Этот способ основан на простом переборе возможных вариантов паролей [2]. Обычно такой перебор выполняется автоматизировано специальной программой. Для уменьшения вероятности подбора пароля почтовые сервисы вносят минимальное количество символов и требуют использование цифр и букв в паролях своих пользователей.

Электронная почта с web-интерфейсом очень удобна для использования в любом месте, где есть компьютер и интернет. Многие web-серверы предлагают сохранить данные настроек, логинов и паролей для того, чтобы при следующем посещении ресурса не пришлось заново вводить все эти данные. Эти данные хранятся на компьютере, с которого произошло подключение и у них есть свое название Cookies. Получив файл сессии и установив его у себя, злоумышленник тем самым обманет сервер, поскольку последний будет считать взломщика настоящим пользователем почтового аккаунта и даст полный доступ. Этот способ можно назвать кража сессии cookies. Для защиты от него является внимательность, на любом почтовом сервере есть функция «Выход», после использования почты необходимо её использовать. Так же возможно удалить запись cookies для ресурса в свойствах обозревателя, т.е. браузера который использует пользователь.

Взлом с помощью ложной страницы, на жаргоне называется фейк. Fake в переводе с английского означает хитрость, обман, мошенничество. Данный способ заключается в создании специальной web- страницы, абсолютно схожей с формой входа на определённом почтовом сервере, и размещении ее в интернете со схожим названием почтового сервера. Затем злоумышленники отсылают письма, где просят перейти по ссылке, по какой либо причине. Перейдя по ссылке пользователь увидит привычную для себя форму входа на почтовый аккаунт и после того как он введет свой логин и пароль, по привычке нажмет кнопку «Вход», злоумышленники получат все необходимые данные. Поэтому всегда проверяйте ссылки, по которым вас просят перейти и тем более, где необходимо вводить пароль.

Как следует из статьи возможность, получения конфиденциальной информации наиболее высока через почтовые сервисы. Способов получения конфиденциальной информации на почтовом ящике очень много и все они очень разные. Выше были рассмотрены способы получения неправомерного доступа, к электронной почте зависящие от пользователя. И если вы их знаете, то вероятность защититься намного выше.

Skype более безопасный способ связи, но тут появляются другие сложности с ограничением использования.

Библиографический список

1. Web сайт посвященный информационной безопасности и защите информации [Электронный ресурс] – Режим доступа – http://all-ib.ru/

2. Википедия [Электронный ресурс] – Режим доступа – http://ru.wikipedia.org/wiki/Skype

3. Злоумышленниками взломана почта советников президента Сирии [Электронный ресурс] – Режим доступа – http://antivibest.ru/page/antivirus-news-223

4. Сайт компании Searchinform, разработчика программных продуктов по защите информации [Электронный ресурс]. – Режим доступа – http://www.searchinform.ru/

5. Статья «Вся правда о Skype» [Электронный ресурс] – Режим доступа – http://freeangels.ucoz.ru/publ/1-1-0-4

6. Статья Хакер заявляет, что сумел взломать протокол Skype [Электронный ресурс]. – Режим доступа – http://ria.ru/technology/20110603/383779119.html

О.О. Голубева

ТРАДИЦИИ И НОВАЦИИ: СИСТЕМЫ МАРКИ «КОДЕКС» И «ТЕХЭКСПЕРТ» В ДЕЯТЕЛЬНОСТИ ВУЗА (ИЗ ОПЫТА РАБОТЫ СЕКТОРА ПРАВОВЫХ БАЗ ДАННЫХ РЦНИТ ПЕТРГУ)

Olga.Golubeva@karelia.ru

Петрозаводский государственный университет, Петрозаводск

The article is devoted to the introduction of electronic systems in the learning process of the Petrozavodsk State University.

Электронные правовые и нормативно-технические системы марки «Кодекс» и «Техэксперт», разрабатываемые Консорциумом «Кодекс», - одного из признанных лидеров российского IT, - давно зарекомендовали себя среди специалистов различных сфер деятельности как в России, так и за ее пределами. Системы «Кодекс» и «Техэксперт» насчитывают более 50 специализированных систем для юристов, экономистов, бухгалтеров, строителей, проектировщиков, экологов, кадровиков и т.д. В настоящее время Консорциум «Кодекс» активно сотрудничает с высшими учебными заведениями. Среди них — Петрозаводский государственный университет. Практически все факультеты и кафедры университета имеют свободный доступ к системам правовой и нормативно-технической документации. Специалисты сектора правовых баз данных РЦНИТ ПетрГУ являются одновременно и «кураторами» работы информационных систем, осуществляя их сопровождение и контроль, и создателями собственных информационных региональных разработок. Специалисты сектора работают над созданием уникальной, лучшей по оценкам экспертов в республике, базы данных «Законодательство Республики Карелия».

С июня 2011 года на сайте http://kodeks.karelia.ru в свободном доступе информационная система "Законодательство Республики Карелия", кодексы Российской Федерации. На сервере юридического факультета установлены системы: «Помощник юриста. Профессионал», «Банк арбитражной судебной практики округов России», программный комплекс «Судебный аналитик», «Банк законодательства регионов России». В сети строительного факультета системы нормативно-технической документации - "Строительное производство и проектирование» и «Техэксперт: Стройтехнолог». На лесоинженерном и агротехническом факультетах — системы «Машиностроение» и «Техэксперт: Экология. Проф».