ТЕХНИЧЕСКИЕ НАУКИ

Гуримская Ирина Анатольевна
старший преподаватель
Ямилев Радик Радикович
студент

Технический институт (филиал)
ФГАОУ ВПО «Северо-Восточный федеральный
университет им. М.К. Аммосова»
г. Нерюнгри, Республика Саха (Якутия)

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ УЧЕБНОГО УЧРЕЖДЕНИЯ

Аннотация*: в статье рассмотрены различные возможные сетевые угрозы для учебного заведения. Авторы рассматривают комплекс мер для обеспечения необходимой безопасности сети.*

Ключевые слова*: сетевая безопасность, сетевые угрозы, сетевые подключения, сетевые ограничения.*

Благодаря развитию IT технологий, большому значению сети в жизни современного человека и общей тенденции к развитию коммуникационных сетей, возникает необходимость создавать в образовательных учреждениях подходящие для обучения условия. Большое количество учебных материалов, различных научных статей и прочих необходимых для обучения знаний все проще и проще найти в сети, нежели в библиотеках. Большинство институтов и школ так же озабочены созданием и поддержкой собственных электронных библиотек, к которым возможен доступ благодаря сети. Множество обучающих курсов, которые помогут обучающимся повысить и закрепить свой уровень знаний, так же находятся в сети.

Ввиду всех этих условий возникает необходимость обеспечить доступ к сети в классах и аудиториях. Но также это делает уязвимым любую информацию,

а также компьютерное оборудование, которым обладает учебное учреждение. Что делает защиту информационной безопасности одном из приоритетных направлений для работы.

Доступ к сети может предоставляться с помощью точек Wi-Fi, либо же через подключения устройства через LAN точку доступа. Угрозы начинают появляться уже на этом этапе. Учащийся, со злым умыслом или же по незнанию, а также из-за желания развлечься во время учебного процесса, может посещать вредоносные или бесполезные сетевые ресурсы. Для устранения этой угрозы необходимо на сервере учебного заведения, через который обеспечивается доступ к сети на остальных устройствах, создать реестр разрешенных и запрещенных сетевых адресов. Например – доступ имеется лишь к образовательным порталам, которые необходимы в процессе обучение, тогда как на другие порталы зайти не имеется даже возможности.

Учащийся так же может пожелать установить на учебные устройства приложения. Это могут быть как компьютерные игры, которые не несут угрозы безопасности как таковой, но также это может быть вредоносное ПО, которое имеет различную классификацию и возможности: от считывания конфиденциальной информации на других устройствах существующей сети до нанесения серьезного ущерба компьютерному оборудованию. Для устранения этой угрозы необходимо ограничить права для пользователей на сетевых устройствах. В результате пользователь не будет иметь возможности внести какие-либо изменения в систему, а сможет лишь пользоваться уже существующим функционалом.

Использование только лицензионного программного обеспечения в работе очень сильно повышает степень защиты устройства. Так же, любое пиратское (взломанное) ПО, во время работы может дестабилизировать состояние системы, причем сделать это невидимо для глаз пользователя. Это зачастую носит длительный характер и несет угрозу лишь в дальнейшей перспективе.

Так же учащийся имеет возможность подключить к общей сети образовательного учреждения собственное сетевое устройство, будь то ноутбук или же мобильный телефон. Это может оказаться так же безобидным действием, но

несет и угрозу в определенных случаях. Допустим на устройстве учащегося, без его ведома, могут содержаться вредоносное ПО которое может начать распространяться по всей существующей сети, к которой оно получило доступ после подключения. Для устранения этой угрозы достаточно на сетевом сервере запретить открывать доступ к сети ново подключенным устройствам. Выглядит это следующим образом – сервер хранит у себя IP-адреса уже подключенных устройств, доступ для которых автоматически открывается. При появлении в списке нового сетевого устройства, а, следовательно, и нового IP-адреса, доступ для этого устройства к сети автоматически закрывается.

Однако, возможна ситуация, что образовательное учреждение позволяет своим учащимся пользоваться своими устройствами, такими как ноутбуки. Тогда, для ограничения доступа к сети нежелательных устройств, есть возможность ограничить доступ по MAC-адресу устройства (у каждого устройства он уникален и в единственном количестве в конкретной компьютерной сети), заранее внеся в список MAC-адреса устройств учащихся.

Вполне очевидным и необходимым так же является установка и стабильное обновление антивирусного программного обеспечения на каждое сетевое устройство – это поможет реагировать на различные угрозы в режиме online.

Если же угрозу предотвратить не удалось и был нанесен ущерб информационному фонду учреждения – на этот случай следует иметь всегда под рукой лицензионное программное обеспечение, которое позволяет восстанавливать поврежденную информацию, а также более комплексные комплексы защиты для лечения системы, ведь исправить сложившуюся ситуацию, как правило, сложнее, чем её предотвратить.

Список литературы

1. Online-курс «Безопасность в интернете». Академия Яндекса [Электронный ресурс]. – Режим доступа: https://stepic.org

2. Безмалый В.Ф. Чем нас пытаются взломать (Краткий обзор программ-взломщиков паролей) / В.Ф. Безмалый, Е.В. Безмалая, 2006.