ТЕХНИЧЕСКИЕ НАУКИ

Аюбова Марет Альвиевна
студентка
Институт информационных технологий и телекоммуникаций
филиала ФГАОУ ВПО «Северо-Кавказский федеральный
университет» в г. Пятигорске
г. Пятигорск, Ставропольский край

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

***Аннотация**: в данной статье автор поднимает актуальную проблему информационной безопасности и рассматривает способы её защиты. Проанализировано понятие «информационная безопасность». Представлено разделение видов защиты информационных технологий и систем накопления информации. Подчеркнута значимость использования антивирусной программы.*

***Ключевые слова**: антивирусная программа, информационная безопасность, информационные технологии.*

На современном развития информационных технологии, система накопления информации, а так же её передача вызывает ряд угроз. Эти угрозы связаны с потерей информации, раскрытия важной конфиденциальной информации. Поэтому обеспечение её безопасности является первоочередной задачей в данной сфере. Цель: рассмотреть понятие информационной безопасности и способов её защиты. В связи с активным внедрение в жизнь человека информационных технологий, увеличился объем информации хранящихся на носителях в электронном виде. Так же и увеличилось число злоумышленников, которые хотят получить данную информацию любым способом. Благодаря появление сети, стало не обязательным находится рядом с компьютером, для получение желаемой информации.

Основываясь на вышесказанном, всё больше стало появляться специальных средств, чтоб защитить надлежащим образом информацию. Одним средством защиты нельзя получить 100 процентную уверенность, что информация не будет подвергнута действиям злоумышленников. В данный момент организации заинтересованы в сохранении тайны о своей деятельности.

Под информационной безопасностью следует понимать процесс защиты от незаконного вторжения, изменения, удаления объектов защиты информации. Достигается безопасность путём обеспечения конфидециальности. К конфидециальности относятся различная личная информация пользователей, пароли, логины, кредитные данные, различные документы, бухгалтерские сведения. Подобная информация может быть доступна только пользователям, которые имеют права на неё. Это могут быть определенные пользователи, программы и иные субъекты системы. Для иных субъектов данные должны быть закрыты. На права к доступа относятся право на чтение, редактирование, копирование, удаление, использование.

Увеличение количества применения информационных технологий даёт возможность и увеличить средства защиты информации. Выбрав доступные, качественные меры, можно защитить организацию от проникновения злоумышленников, от порчи, удаления, кражи информации любого типа.

Меры защиты можно разделить на несколько видов, такие как, правовые, технические, физические, технологические, организационные. Основной мерой защиты информации является правовая и техническая. Правовой защитой является разработка законодательных актов, которые регулируют отношения по защите информации. Функцией подобной меры защиты является предотвращение совершения преступлении в области разглашение информации. Основным источником защиты информации у нас в стране является Конституция РФ, а законодательным материалом является ФЗ «Об информации, информатизации и защите информации». Данный закон является разграничением информационных ресурсов по категориям, прописывает цели защиты информации.

К технической защите информации можно отнести применение различных технических средств, программ. Подобная мера защищает от любого внешнего воздействия, от вирусов, от кражи информации. Очень распространенная техническая защита от вирусов, которые просто заполонили Интернет. Практически в каждой организации, каждый пользователь использует мощные антивирусные программами. Так же сформулированы определенные правила, которые необходимы при пользовании компьютерами. Для улучшения работы данной системы стоит оснастить каждое рабочее место основными правилами защиты от вредоносных программ. В данные правила можно отнести: постоянная проверка внешних носителей; ежедневная проверка компьютера на наличие вредоносных программ, использование только проверенных антивирусных программ; не пользоваться сомнительными сайтами; не открывать сомнительные файлы, которые приходят на электронную почту. Каждый сотрудник приступая к работе должен быть подробно ознакомлен с подобной техникой безопасности.

Так же нужно обязательно обратить внимание и на антивирусную программу, которой оснащаются персональные компьютеры. Такая программа должна постоянно проводить защиту оперативной памяти. Программа должна как автоматически, так и по требованию пользователей проводить тестирование поступающей информации на компьютер. Регулярное обновление антивирусной базы, так же является неотъемлемой частью антивирусной программы. Так как ежедневно создаются множество вредоносных программ, которые влияют на качество поступающей информации и работу системы. Программа по мимо контроля поступающей информации должна уметь лечить и удалять найденные вирусы.

Набор средств информационной защиты в каждом предприятии должна быть стандартна и соответствовать следующим пунктам:

– Использовать средства защиты на файловом уровне.

– Использовать качественные, лицензионные антивирусные программы.

– Использование ключей, смарт-карт.

– Применять средства обеспечения централизованного управления системой информационной безопасности.

– Не передавать информацию, которая является конфидециальной другим лицам.

– Проводить постоянные беседы с работниками о соблюдении правил конфидециальности.

– Ограничить права доступа к объектам.

– Создание индивидуального технического системного программного обеспечения для более надежного использования.

Таким образом, для успешной зашиты информации, и для предотвращения проникновения злоумышленников достаточно применять ряд мер защиты, контролировать из исполнение, проводить регулярно профилактические меры среди сотрудников.

Список литературы

1. Конституция Российской Федерации. – М.: Проспект, 2015. – 30 с.

2. Горбенко И.Д., Качко Е.Г., Потий А.В. Решения и средства защиты информации. – М.: Форум–ИнфраМ, 2004. – 528–533 с.