Муниципальное бюджетное общеобразовательное учреждение
среднего общего образования «школа №2 г.Облучье»

Научно - практическая конференция

"Обеспечение и роль информационной безопасности в современном мире"

Автор проекта: ученик 9 класса А
Щегорцов Александр ергеевич

Руководитель: Бугрештанова Мария Геннадьевна, учитель информатики

г.Облучье 2019

Введение

К написанию данной работы меня натолкнул прогремевший на весь мир поступок технического специалиста ЦРУ Эдварда Сноудена.

Он рассказал всему миру о том, как «присматривают» за всем миром власти США, Британия и их программах PRISM и TEMPORA.

Сноуден раскрыл информацию о программе PRISM, включающей в себя массовую слежку за переговорами американцев и иностранных граждан посредством телефона и Интернета. PRISM позволяет Агентству просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, узнавать другие подробности из социальных сетей

Наверняка, вы могли подумать, что обычных «юзеров» Интернета это не коснулось, но вы глубоко ошибаетесь.

В программе PRISM принимают участие такие известные компании как Microsoft (Hotmail), Google (Gmail), Apple, YouTube, Skype.

Все заметили знакомые названия?

Все эти корпорации следили за своими пользователями по всему миру с помощью встроенного интегрированного программного обеспечения.

Проблема обеспечения информационной безопасности в рамках любого государства в последнее время все чаще является предметом обсуждения не только в научных кругах, но и на политическом уровне. Данная проблема также становится объектом внимания международных организаций, в том числе и ООН.

Информационное воздействие стало главным рычагом управления людьми, заменив физическое воздействие, тысячелетиями считавшееся непременным

средством управления. Поэтому одним из основных элементов национальной, общественной и личной безопасности становится информационная безопасность.

В современном мире информационная безопасность – жизненно необходимое условие обеспечения интересов человека, общества и государства. **Целью данной работы** является исследование основных принципов и направлений обеспечения информационной безопасности

Актуальность работы заключается в том, что в наше время нужно уметь сохранять конфиденциальную информацию,т.к она считается жизненно-весомым аспектом.

Новизна работы в том, что в рамках школьных исследовательских работ не поднималась тема информационной безопасности.

В рамках данной цели были поставлены следующие задачи:
1. Изучить литературу по данному вопросу

2.Познакомиться с основными принципами и направлениями обеспечения информационной безопасности.

3.Выяснить, на сколько осведомлены ученики нашей школы в плане информационной безопасности

В ходе решения вышеуказанных задач были использованы следующие **методы исследования:**

1. Знакомство с научной литературой по данной теме
2. Поиск информации в сети Интернет
3. Проведение опроса среди учащихся школы
4. Анализ полученной информации.

Гипотеза исследования: предположим, что информационная безопасность играет важную роль в современном мире это придаёт ей большее значение и важность, но ученики нашей школы недостаточно осведомлены в плане ИБ.

<u>История информационной безопасности</u>

Объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесён ущерб путём воздействия на средства информационных коммуникаций.

Информация - это любые **сведения**, принимаемые и передаваемые, сохраняемые различными источниками. *Информация* - это вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системами.

Информация необходима каждому как условие и как средство существования человека в обществе, поэтому так же нуждается в защите, как и все остальные элементы жизнедеятельности. Современный этап развития общества характеризуется возрастающей ролью электронных ресурсов, представляющих собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

Стремительный рост компьютерных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения в этих сферах, а с другой стороны, стал источником самых непредсказуемых и вредных для человеческого общества последствий. В результате, можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях.

Очень быстро компьютеры были объединены Интернетом, что привело к взрывному росту электронного бизнеса. Всё это, в сочетании с появлением киберпреступности и множеством случаев международного терроризма, вызвало

потребность в лучших методах защиты компьютеров и информации, которую они хранят, обрабатывают и передают.

Основные цели информационной безопасности.

Основные принципы ИБ были сформированы Джерри Зальцером и Майклом Шрёдером.

Их разделили на 3 основные категории:

***C**onfidentiality* Конфиденциальность

***I**ntegrity* Целостность

***A**vailability* Доступность

В совокупности эти три ключевых принципа информационной безопасности именуются ***триадой CIA.***

В 1992 году ОЭСР опубликовала свою собственную модель информационной безопасности, состоящую из девяти принципов: осведомлённость, ответственность, противодействие, этика, демократия, оценка риска, разработка и внедрение безопасности, управление безопасностью, пересмотр. В 1996 году на основе публикации ОЭСР 1992 года американский Национальный институт стандартов и технологий (NIST) сформулировал восемь основных принципов, которые гласят, что компьютерная безопасность «поддерживает миссию организации», «является неотъемлемой составляющей рационального менеджмента», «должна быть экономически эффективной», «требует всеобъемлющего и комплексного подхода», «ограничивается социальными факторами», «должна периодически подвергаться пересмотру», «обязанности и ответственность за компьютерную безопасность должны быть чётко сформулированы», а «владельцы систем несут

ответственность за безопасность за пределами своей организации». На основе этой модели в 2004 году NIST опубликовал 33 принципа инженерного проектирования систем информационной безопасности, для каждого из которых были разработаны практические руководства и рекомендации, которые по сей день постоянно развиваются и поддерживаются в актуальном состоянии.

Основные задачи информационной безопасности

Обеспечение информационной безопасности требует решения целого комплекса задач. *Важные из них:*

разработка основных направлений государственной политики в области обеспечения информационной безопасности, а также мероприятий и механизмов, связанных с реализацией этой политики;

развитие и совершенствование системы обеспечения информационной безопасности, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности, а также системы противодействия этим угрозам;

разработка федеральных целевых программ обеспечения информационной безопасности;

разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности, а также их сертификации;

совершенствование нормативно-правовой базы обеспечения информационной безопасности;

установление ответственности должностных лиц федеральных органов власти и местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;

координация деятельности органов государственной власти, предприятий, учреждений и организаций независимо от форм собственности в области обеспечения информационной безопасности;

развитие научно-практических основ обеспечения информационной безопасности с учетом современной геополитической ситуации, условий политического и социально-экономического развития и реальности угроз применения информационного оружия;

создание механизмов формирования и реализации государственной информационной политики;

повышение эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, прежде всего в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

развитие и совершенствование систем защиты информации и государственной тайны;

создание защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

расширение взаимодействия с международными и зарубежными органами и организациями для обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

создание системы подготовки кадров в области информационной безопасности и информационных технологий.

Основные направления обеспечения информационной безопасности.

Правовая защита- это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

Организационная защита- это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;

Инженерно-техническая защита- это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

Также можно выделить такие направления как:

Защита каналов связи (телекоммуникационная безопасность)

Эксплуатационная безопасность

Безопасность сетей

Информационная безопасность

Компьютерная безопасность

Защита от ПЭМИН (побочные электромагнитные излучения и наводки)

Безопасность персонала (защита от персонала)

Физическая безопасность

Административная безопасность

Принципы обеспечения информационной безопасности.

Принципы:

Системности

Комплексности

Неразрывной защиты

Разумной достаточности

Гибкость управления и применения

Простоты применения защитных мер и средств

Принцип системности.

Системный подход к защите компьютерных систем предполагает необходимость взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления.

При обеспечении ИБ ОС необходимо учитывать все слабые и наиболее уязвимые места системы, а так же характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения распределенной системы и НСД к информации.

Принцип комплексности.

Для обеспечения защиты имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты,

перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов.

Принцип непрерывности защиты.

ЗИ это не разовое мероприятие и не конкретная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный направленный процесс предполагающий принятие соответствующих мер на всех этапах существования АС. Разработка системы защиты должна вестись параллельно обработке самой защищаемой системы.

Разумная достаточность.

Важно правильно выбрать тот уровень защиты при котором затраты риск и размер возможного ущерба были бы приемлемы и не создавали неудобств пользователю.

Гибкость системы защиты.

Часто приходится создавать систему защиты в условиях большой неопределенности поэтому принятые меры и средства защиты особенно в начальный период их эксплуатации могут оказывать как чрезмерный так и недостаточный уровень защиты. Для обеспечения уровня варьирования защищенности средство защиты должно обладать определенной гибкостью особенно если средство необходимо установить на работающую систему не нарушая процесса её нормального функционирования.

Принцип простоты применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких либо языков или требовать дополнительных затрат на её применение, а так же не должно требовать выполнения рутинных малопонятных операций.

Заключение

Моя гипотеза не подтвердилась, так как наши ученики достаточно осведомлены в плане ИБ. В ходе данной исследовательской работы были рассмотрены цели, задачи, принципы и основные направления обеспечения информационной безопасности, а так же проверили пользуются ученики нашей школы принципами защиты, а именно принципом системности, гибкостью системы защиты, принципом комплексности.

Информационные технологии дали нам возможность использования приемов, моделирующих интеллектуальную деятельность человека, для создания средств производства и предметов потребления, ведения вооруженной борьбы, обеспечения социальной коммуникации. По мере развития научно-технического прогресса, возрастания роли информационных технологий в повседневной жизни, их проникновения во все сферы деятельности общества и государства, все большее значение приобретает информационная безопасность личности. Я считаю, что курс ИБ должен проводиться на всех ступенях образования, чтобы ученики нашей школы научились безопасно распоряжаться информацией.