Куликова Ирина Геннадьевна
старший преподаватель
ФГБОУ ВО «Самарский государственный
университет путей сообщения»
г. Самара, Самарская область
Куликова Полина Сергеевна
студентка
ФГАОУ ВО «Самарский национальный исследовательский
университет им. академика С.П. Королева»
г. Самара, Самарская область

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К вопросу об информационной безопасности

Аннотация: *в статье проанализированы наиболее распространенные интернет-мошенничества, представленные в киноиндустрии, и предложены методы борьбы с ними с применением технологий информационной безопасности.*

Ключевые слова: *информационные технологии, информационная безопасность, защита информации, кибер-атаки, компьютерный вирус.*

Втягиваясь все более в виртуальный мир, человечество не протестует против окружения своей жизни компьютерами на работе, в быту. Это объяснимо. Ведь информационные технологии помогают нам в решении огромного количества различных задач, в обработке информации за невероятно короткое время, в работе с видео и аудиоинформацией.

К сожалению, нынешний век с уверенностью можно обозначить не только как век инновационных информационных технологий, но и как век интеллектуальных информационных войн. Человечество принимает необходимость всеобщей компьютеризации и применения информационных техно-

логий в своей жизни, и этим активно пользуются нечистоплотные представители информационного мира. От информации сегодня зависит как работа предприятия или отдельного пользователя в принципе, так и его конкурентоспособность. Поэтому деятельность по защите информации, по обеспечению информационной безопасности в настоящее время представляется очень значимой.

Для проведения анализа наиболее распространенных интернет – мошенничеств, представленных в киноиндустрии, был выбран фильм «Мистер робот» о мошенничествах хакера Эллиота Алдерсона. Рассмотрим с позиций информационной защиты схемы, которые использует герой с целью разрушения корпораций.

Одним их наиболее важных условий информационной безопасности является выбор личного пароля. Герой фильма Эллиот легко взламывает почту своего психотерапевта. Пароль героини был очень прост, он состоял из имени любимого певца и года ее рождения, расположенных наоборот — Dylan_2791. Пароли, состоящие из значимых для нас имен и дат, совершенно не надежны. Преступник легко его разгадывает, потратив время на перебор вариантов. Единственный надежный способ сохранить пароль в тайне — сделать его непростым и менять как можно чаще.

В целях собственной безопасности не следует откровенничать с незнакомыми. Обладающий необходимыми навыками хакер способен узнать нужную информацию. Так Эллиот выясняет маршрут такси с нужным человеком, элементарно солгав диспетчеру по телефону, что в автомобиле утеряны ключи. И в ответ получает необходимый адрес. Потому перед тем, как рассекретить свои данные, следует заставить звонящего представиться и объяснить, для чего эти данные потребовались. Пароль же сообщать по телефону не следует категорически.

Гражданам, активно использующим интернет-технологии необходимо соблюдать цифровую гигиену. Надо помнить, что бесплатно — не означает безопасно. В фильме герой устанавливает вирус на компьютер собеседника,

презентовав ему бесплатный промо-диск с музыкой. Подобный вирус способен передавать сведения о действиях владельца компьютера хозяину вируса. Последствиями станут утечка информации, беззастенчивое скачивание и уничтожение личных данных и даже возможный последующий шантаж. Как бороться с вирусом? Делать резервные копии. Тогда вирус не столь опасен, документы можно восстановить.

Цифровая гигиена предполагает также: не подключение к компьютеру устройств, в которых нет уверенности, не скачивание файлов с сомнительных сайтов и хранение в свободном доступе только данных, не несущих конфиденциальную информацию.

Следует держать при себе свою технику и телефон. Появилась масса приложений, отслеживающих чужие мобильные телефоны. Устанавливать их следуют крайне осторожно. Не будьте беспечны, используя «Википедию». Чтобы попасть в хранилище данных, Эллиот подделывает страницу в «Википедии». Преступники просто копируют известные сайты, доверчивый пользователь вводит данные карты, и они поступают к преступнику. Поэтому необходимо следить за правильным написанием адресов сайтов, которыми пользуешься: не откликаться на cbrehbank вместо Сбербанк, на vtentakle вместо верного названия соцсети.

Может ли рядовой пользователь защититься от хакерских атак? Безусловно, может. Следует ответственнее относиться к своей безопасности в сети, чаще менять пароли, обновлять антивирусы. Утверждение нового цифрового пространства – это будущее, которое выстраивается на наших глазах. И которое утвердится непременно. И потому хочется воспринимать все, что связано с информационным пространством, позитивно.

Список литературы

1. Куликова И.Г. Информационная модель системы образования [Текст] / И.Г. Куликова, П.С. Куликова, И.Ю. Евдошенко // Современное образование в России и за рубежом: теория, методика и практика: Материалы V Междунар.

науч.-практ. конф. (Чебоксары, 31 дек. 2016 г.) / Редкол.: О.Н. Широков [и др.]. – Чебоксары: ЦНС «Интерактив плюс», 2016. – С. 200–202.