МИНЕСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧЕРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Практическая работа №2

По дисциплине «Основы защиты информации»

За 3 семестр

Тема: «Угрозы информационной безопасности»

Выполнили:

студентки 2 курса

группы АС-56

Казак А.А.

Карпенко М.В.

Проверил:

Безобразов С.В.

Брест 2020

*Задание 1:* Для выбранного объекта защиты информации привести всевозможные угрозы информационной безопасности в рамках разновидностей этих угроз.

*Задание 2:* Привести классификацию перечисленных угроз по ряду базовых признаков.

*Объект*: планшет.

*Задание 1:*

Угроза безопасности - потенциально возможное событие, действие, процесс, которое может привести к нанесению ущерба чьим-либо интересам - искажение, уничтожение, копирование, а также возможность воздействия на компоненты автоматизированной системы.

Разновидностями этой угрозы являются:

* Угрозы нарушения конфиденциальности
* Угрозы нарушения целостности
* Угрозы отказа служб

Для выбранного нами объекта наиболее актуально две из трёх угроз, а именно:

* Угроза нарушения конфиденциальности

Первое, что является основой нарушения конфиденциальности - это перехват данных, кража логинов, паролей, аккаунтов пользователей. Перехват данных - очень серьезная угроза, и, если конфиденциальность действительно критична, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Так, при неосторожном скачивании файлов с интернета пользователь может совершенно случайно либо скачать на планшет вирус, либо разрешить доступ к своим конфиденциальным данным. В случае неосторожной загрузки вируса последствия могут быть самыми непредсказуемыми. Мошенники маскируют вирусы под безобидные приложения и файлы: браузеры, плееры, игры, навигаторы, книги, антивирусы. Затем они распространяют их: например, ищете в интернете какую-нибудь игру или программу, и попадаете на форум. Кто-то оставил нужную ссылку и все дружно его благодарят. На самом деле форум и комментаторы не настоящие. Или, заходя на сайт с пиратскими фильмами и сериалами, появляется сообщение. В нем написано, что планшет заражен вирусами или какая-то программа сильно устарела. Бывает даже так, что устройство начинает вибрировать или издавать странные звуки. На самом деле это не так и с устройством все в порядке. Или второй вариант, по SMS или электронной почте. Как правило, это SMS с сайтов бесплатных объявлений, письма от «нотариусов из Германии», сообщения о выигрыше в лотерею. Нужно быть осторожным, в большинстве случаев это мошенники. У всех подобных сообщений общая цель – заставить нажать на ссылку, чтобы вирус скачался на устройство.

Таким образом нужно быть внимательным, скачивать и пользоваться приложениями из надежных источников. Это гарантия того, что приложения является легитимными.

* Угрозы отказа служб

Угроза отказа служб возникает всякий раз, когда в результате преднамеренных  действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. На разных уровнях доступа к информации угроза отказа служб может быть разной. Так, например, может быть выведен из строя носитель информации (в нашем случае - планшет), могут проявляться ошибки проектирования или разработки, искажения соответствия синтаксических и семантических конструкций языка, либо запрет на использование информации. Снова можно говорить об аккуратном обращении с интернет-сайтами, так как пользователи, в большинстве случаев, использую планшеты для просмотра и скачивания информации с сети.

* Угрозы нарушения целостности

Это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. В наше время использование планшетов не так актуально, как использование телефонов (смартфонов), либо компьютеров, поэтому велика вероятность того, что наиболее важные данные пользователя хранятся на других устройствах. Исходя из этого можно сделать вывод, что это угроза менее актуальна, чем все остальные.

*Задание 2:*

Классификация угроз безопасности имеет множество подпунктов, но мы остановимся только на тех, которые касаются нашего объекта информации – планшета. По природе возникновения. Делятся на угрозы среды и угрозы, обусловленные человеческим фактором. К угрозам среды (естественным) относятся угрозы, возникшие в результате явлений, не зависящих от человека, к примеру, природных и стихийных. Здесь необходимо отметить, что самой неприятной особенностью таких угроз является невозможность их прогнозирования. В свою очередь, угрозы, связанные с проявлением человеческого фактора, могут различаться по способу осуществления: случайные или целенаправленные (преднамеренные). Случайные (непреднамеренные) угрозы могут быть связаны с различными ошибками, например: с ошибками пользователей при работе в системе. Другая же группа, чаще всего связана с алчными целями, целями материальной выгоды или даже моральными предубеждениями злоумышленников. Можно классифицировать угрозы по степени воздействия на системы (характеру угрозы) и по способу доступа к защищаемым ресурсам. По степени воздействия различают пассивные и активные угрозы. Пассивные, в случае реализации не вносят каких-либо изменений в состав и структуру системы, к примеру, копирование и хищение конфиденциальной информации. Активные же угрозы, оказывают влияние на работу системы, в частности примером такой угрозы является «Отказ в обслуживании». Остальные угрозы, по нашему мнению, больше применимы к работникам каких-либо систем и организаций, а не к простым пользователям.

*Вывод:*

Для выбранного объекта защиты информации привели всевозможные угрозы информационной безопасности в рамках разновидностей этих угроз, привели классификацию перечисленных угроз по ряду базовых признаков. Сделали вывод о том, что пользователь должен быть осторожен при пользовании интернетом, а также о том, что более осторожными должны быть работки организаций, по причине того, что для злоумышленников информация фирм и компаний важнее, нежели данные простых пользователей.