Министерство образования Республики Беларусь

Учреждение образования

Брестский государственный технический университет

Кафедра ИИТ

Практическая работа №3

По дисциплине ОЗИ

Выполнили:

Студенты ФЭИС

Группы ПО-4

Иваненко И.Л.,

Елисеев С.Г.

Проверил:

Безобразов С.В.

Брест 2020

Практическая работа №3

Типы злоумышленников

Цель: для выбранного объекта защиты информации(PayPal) разработать типы предполагаемых злоумышленников. Предоставить описание их вероятных действий, классифицировать по степени опасности.

Ход работы:

1. Типы злоумышленников:
2. Разработчик
3. Сотрудники из числа обслуживающего персонала
4. Пользователь
5. Постороннее лицо

Потенциальная опасностть для каждого из типов злоумышленников уменьшается сверху вниз(Разработчик – самый опасный, Постороннее лицо – наименее опасный)

1. Вероятные действия злоумышленников:

1) Разработчик является наиболее опасным типом злоумышленника, так как он располагает наиболее полной информацией о данном объекте.

Пользователь имеет общее представление о структурах компьютерных систем, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации.

Большие возможности оказания вредительских воздействий на информацию компьютерных систем имеют специалисты, обслуживающие эти системы. Причём, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. В случае преднамеренного или непреднамеренного действия работника обслуживающего систему, система безопасности может быть уязвима в результате чего злоумышленнику легче взломать и украсть данные со страницы пользователя.

Постороннее лицо, не имеющее отношения к компьютерным системам, находится в наименее выгодном положении по отношению к другим злоумышленникам. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если компьютерная система является распределенной. Постороннее может получить доступ к странице в соц. сети в результате заражения компьютера пользователя и получения паролей хранящихся в браузере, также злоумышленник может получить доступ к странице другими способами, и использовать полученную информацию в своих целях.

1. Расположить злоумышленников по степени опасности:
2. Разработчик
3. Сотрудники из числа обслуживающего персонала
4. Посторонний человек
5. Пользователь

Вывод: разработал классификацию злоумышленников для выбранного объекта защиты информации. Рассмотрел возможные действия злоумышленника и расположил злоумышленников по степени опасности.