

СЕКЦИЯ 12 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНСТРУМЕНТАЛЬНЫЕ И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ЭКОНОМИКЕ

В. А. Беженцева, А. А. Кунаш

Научный руководитель – кандидат физико-математических наук
Н. Г. Токаревская
БГЭУ (Минск)

ФИНАНСОВЫЕ КИБЕРМОШЕННИКИ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Количество киберугроз, нацеленных на финансовые операции в сети, постоянно растет, более того, они становятся все сложнее, поэтому тема кибермошенничества в настоящее время весьма актуальна.

Цель данной работы – обзор основных видов компьютерного мошенничества и анализ современных способов защиты от него.

Кибермошенничество – это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получит доступ и каким-либо образом использует личную информацию интернет-пользователя, что предполагает мошенничество или обман. Среди информации, потенциально доступной злоумышленникам в киберпространстве, наибольшей популярностью пользуются финансовые данные. Это закономерно – такую информацию проще всего превратить в деньги, продав на черном рынке либо воспользовавшись ею самостоятельно.

Виды кибермошенничества: нигерийские письма, фишинг, вишинг, фарминг, обман при покупке товара в интернет-магазине, махинации в интернет-аукционах.

Согласно данным «Лаборатории Касперского» в 2013 г. более 63 % пользователей в мире хотя бы раз столкнулись с мошенниками, пытавшимися украсть их персональные данные банковских и платежных онлайн-систем.

В таких условиях специальная защита финансовых операций, совершаемых в Интернете, становится особенно востребованной. Лучшая защита от кибермошенничества – здравый смысл. Если предложение слишком хорошо, чтобы быть правдой, то это скорее всего обман. Киберугрозы постоянно усложняются, поэтому необходима повышенная бдительность и выделение достаточных ресурсов на идентификацию и нейтрализацию соответствующих рисков.

Таким образом, чтобы избежать киберугроз, необходимо:

- не доверять любым нежелательным сообщениям, содержащим просьбу предоставить личную информацию;

- игнорировать спам;
- никогда не предоставлять свои персональные данные людям, в личности которых недостаточно уверены;
- запоминать свои пароли и PIN-коды;
- проявлять осторожность при совершении онлайн-покупок, так как существует угроза фишинга, при которой мошенник может узнать номер кредитной карты (для этого использовать веб-сайты, которые обеспечивают безопасность сделок, ознакомиться с политикой конфиденциальности сайта);
- и самое главное, следует установить и регулярно обновлять программные продукты, обеспечивающие безопасность вашего компьютера (antivirus, antispyware и antimalware), поскольку безопасность должна быть многоуровневой.

Список использованных источников

1. Корпоративные информационные технологии и решения [Электронный ресурс] / PCweeklive. Российская Федерация. – М., 2013. – Режим доступа: <http://www.pcweek.ru/security/news-company/detail.php?ID=158576/>. – Дата доступа: 30.04.2014.
2. Internet and software company [Электронный ресурс] / ed. K. L. Klint. Российская Федерация. – М., 2012. – Режим доступа: <http://www.interface.ru/home.asp?artId=35963/>. – Дата доступа: 30.04.2014.

А. А. Боровская

Научный руководитель – кандидат экономических наук Н. Ф. Корсун
БГАТУ (Минск)

МОДЕЛЬНАЯ ПРОГРАММА РАЗВИТИЯ ЖИВОТНОВОДЧЕСКИХ ОТРАСЛЕЙ НА ПРИМЕРЕ ИЧУСП «ШТОТЦ АГРО-СЕРВИС»

Принятие решений – составная часть любой управленческой функции на предприятии. Необходимость принятия решений возникает на всех этапах процесса управления, где целесообразно использовать экономико-математические методы и модели. Существует ряд причин, обуславливающих создание и использование моделей вместо попыток прямого взаимодействия с реальным миром. К ним относятся естественная сложность многих организационных ситуаций, невозможность проведения экспериментов в реальной жизни и ориентация руководства на будущее [2, с. 24].

Разработка программ развития для конкретного предприятия в наибольшей мере приспособлена к достижению поставленных целей, т. е. максимизации прибыли, и как мощное аналитическое средство позволяет преодолевать множество проблем, связанных с принятием решений в сложных ситуациях.