УДК 658.29-049.5

ИССЛЕДОВАНИЕ СТРУКТУРЫ И ТЕХНОЛОГИЙ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В.В. МАЛИКОВ, Р.В. РАБЦЕВИЧ, С.В. ПУЗЫНА

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
malvvv104@mail.ru

Предложена классификация рынка киберпреступности. Проведено исследование технологий совершения преступлений в системах безналичных электронных платежей сервисов сети Internet.

Ключевые слова: интернет-мошенничество, спам, DDos-атаки, рынок криминальных средств систем и услуг, преступления в системах безналичных электронных платежей.

Глобальный рынок киберпреступности активно развивается и совершенствуется в соответствии с передовыми направлениями информатизации общества, внедрением электронных систем коммуникаций, электронных платежных систем [1].

В ходе исследования проведена декомпозиция рынка киберпреступности на законченные функциональные уровни и модули (рис. 1).

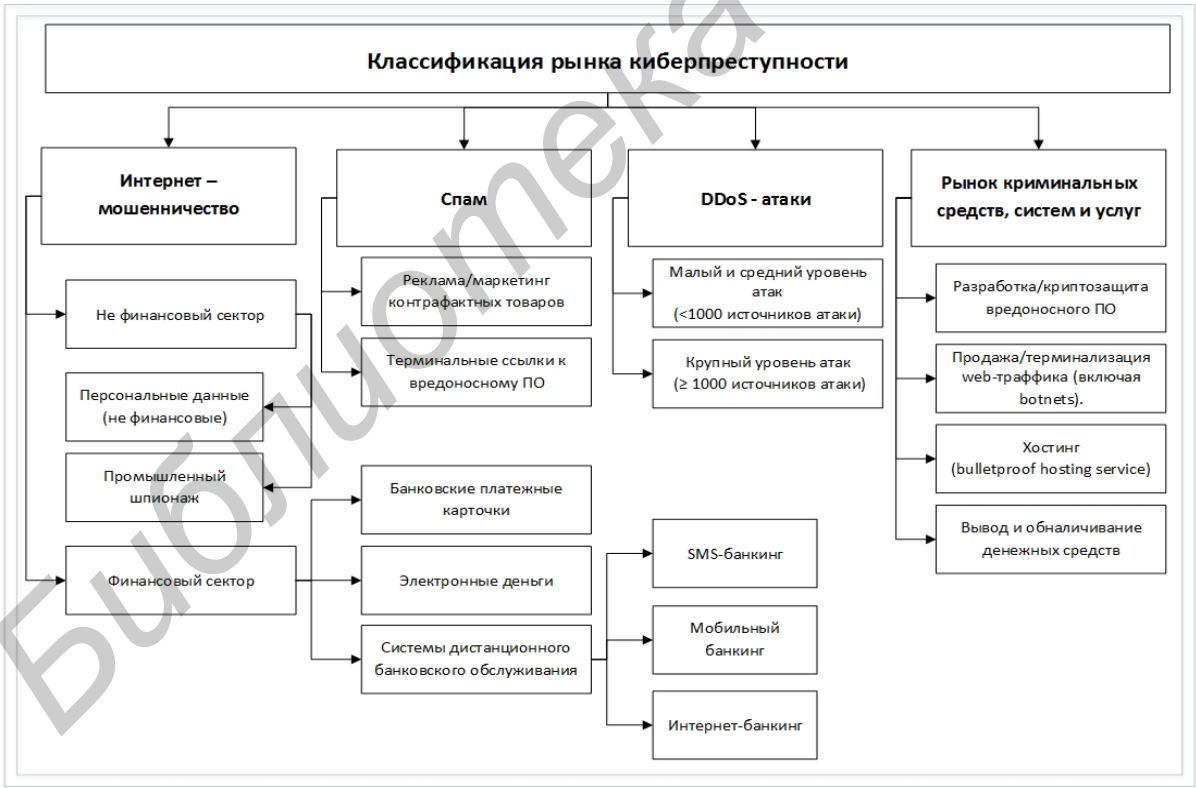

Рис. 1. Классификация рынка киберпреступности

Предлагается использование варианта декомпозиции, который учитывает полный технологический цикл осуществления атак, включающий как разработку вредоносного программного обеспечения, так и непосредственно его использование в преступных целях. В качестве

базовых уровней предлагаются следующие: интернет-мошенничество, спам, DDos-атаки, рынок криминальных средств систем и услуг.

Наибольший интерес для криминального организатора киберпреступлений представляют безналичные электронные платежи пользователей сервисов сети internet [2].

Основные варианты перехвата управления в сервисах безналичных электронных платежей приведены на рис. 2.

Для устранения возможностей перехвата и повышения уровня безопасности платежными сервисами используется алгоритм двухфакторной аутентификации пользователя. Однако, наиболее развитые и технологичные троянских программы, используемых киберпреступниками, например банковский троянец ZeuS (Zbot) совместно с мобильным троянцем ZeuS-in-the-Mobile (ZitMo), могут обходить данную систему защиты Другие системы защиты сервисы безналичных электронных платежей также нейтрализованы киберпреступниками: система chipTAN — банковский троянец SpyEye; система на основе USB-токена — банковский троянец Lurk.

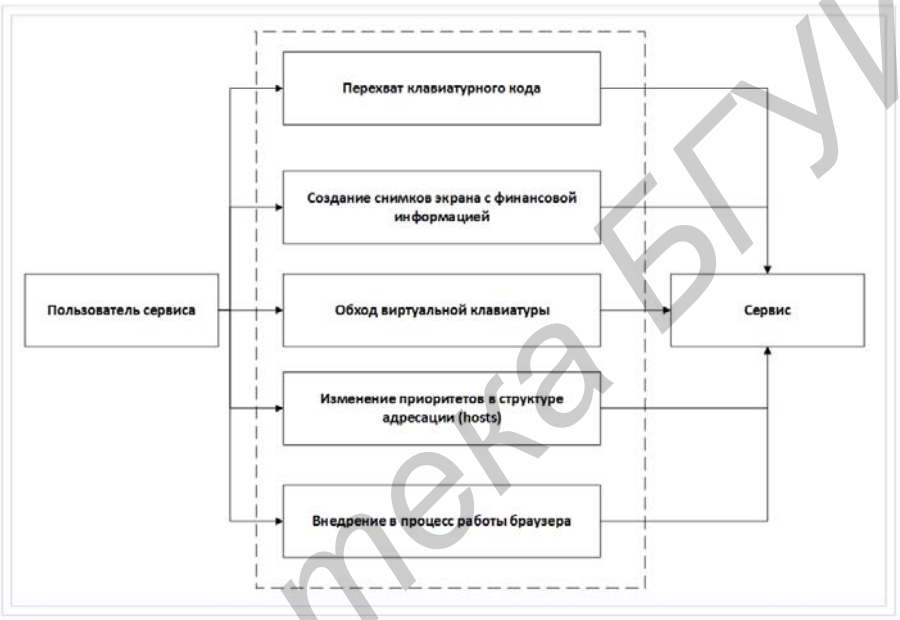

Рис. 2. Схема перехвата управления в сервисах безналичных электронных платежей

Проведение исследования структуры и технологий совершения киберпреступлений позволяет государственным регуляторам и организациям по борьбе с киберпреступлениями оперативно реагировать на инциденты информационной безопасности, формировать методики оперативно-розыскных мероприятий и повышать общий уровень информированности граждан.

Список литературы

1. Рынок преступлений в области высоких технологий: состояние и тенденции 2013 года // group-ib.ru [Электронный ресурс]. – 2013. – Режим доступа: http://www.group-ib.ru/list/1008-analytics/?view=article&id=1155. – Дата доступа: 14.01.2014.

2. Защита от виртуальных грабителей // securelist.com [Электрон. ресурс]. – 1997. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050811/Zashchita_ot_virtualnykh_grabiteley – Дата доступа: 15.01.2014.