УДК 343.9

Глушкова М.П.,
студентка 2 курс,
Институт общественных наук и массовых коммуникаций
Белгородский государственный университет
Россия, г. Белгород
Научный руководитель: Благорожева Ж.А.,
ассистент кафедры «Социологии и организации работы с молодежью»
Белгородский государственный университет
Россия, г. Белгород

ХАКЕРЫ КАК ФЕНОМЕН ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Аннотация: *Защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. По мере развития технологий платежных систем серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. В данной работе исследована проблема хищения личной информации киберпреступниками, также изучены методы борьбы с данным видом мошенников.*

Ключевые слова: *киберпреступник, хакер, информационная война, фишинговые компании, CEIW (информационная война с поддержкой киберпространства).*

Annotation: *Data protection in computer networks is becoming one of the most acute problems in modern computer science. With the development of payment system technologies, a serious failure of local networks can simply paralyze the work of entire corporations and banks, which leads to tangible material losses. In this paper, the problem of theft of personal information by cybercriminals is investigated, and methods of combating this type of fraud are also studied.*

Keywords: *cybercriminal, hacker, information warfare, phishing companies, CEIW (information warfare with cyberspace support).*

На сегодняшнее время социальные сети приобретают все большее значение в формировании общественного мнения, старые добрые времена дезинформации времен холодной войны ушли в прошлое, однако социальные сети являются всего лишь «экологическими палатами». Иностранные субъекты со злым умыслом могут легко использовать эту неотъемлемую особенность социальных сетей, манипулирующих онлайн-информацией, чтобы влиять на общественное мнение. Кроме того, киберпространство обеспечивает высокую степень анонимности, за которой легко автоматизировать пропаганду, и кибератаки могут быть использованы для фильтрации и раскрытия конфиденциального контента или для получения информационного доминирования во время военных операций, повышая стратегическую значимость «информационного пространства». Операции в этой области занимают центральное место в стратегическом мышлении России в области безопасности, главным образом в ее военной доктрине «Война нового поколения». Но продолжающаяся милитаризация киберпространства чревата опасными последствиями в обычной сфере. Что могут сделать главы государств, чтобы защитить открытые демократии, сохраняя при этом глобальный, свободный и устойчивый Интернет? Ответ многогранен, поскольку CEIW является возникающей асимметричной угрозой, которая заставляет правительства во многих отношениях внедрять инновации в подход к безопасности.

Желание влиять на общественные дебаты в зарубежных странах не является чем-то новым, поскольку дезинформация и психологические операции (PSYOP) уже давно являются инструментом в арсенале государств. Что меняется, так это уровень непосредственности, масштабы деятельности и масштабы усилий, прилагаемых к этим операциям, что стало возможным

благодаря все более широкому распространению Интернета и его растущей значимости в формировании общественного мнения. Киберпространство является мощным мультипликатором дестабилизирующих эффектов манипулируемой информации, поскольку оно обеспечивает высокую связность, низкую задержку, низкую стоимость входа, множество точек распространения без посредников и полное игнорирование физических расстояний или национальных границ. Самое главное, анонимность и отсутствие определенной атрибуции атаки делают киберпространство «областью неопределенности».

Эти неотъемлемые особенности киберпространства легко используются иностранными субъектами со злонамеренным намерением распространять поддельные новости и инструктировать платных троллей (каждый из которых контролирует несколько онлайн-профилей) распространять контент, которым манипулируют в Интернете, чтобы обмануть, отвлечь и дезинформировать общественное мнение, разбивая дебаты разноречивыми истинами, которые в конечном итоге дезориентируют и подтверждают чувство сомнения среди общественности или формируют мнение определенной целевой аудитории по определенному вопросу. [5,с.29]

Враждебные субъекты в киберпространстве также готовы и способны использовать множество инструментов, разрешенных компьютерными сетевыми операциями (cNOS) и «компьютерной пропагандой», чтобы влиять на общественное мнение до такой степени, о которой старомодные психологи могли только мечтать. Эти кибер-инструменты позволяют гораздо большее влияние на целевые аудитории, например, создавая практически бесконечный ряд автоматизированных скриптов (ботов), чтобы заполнить социальные сети и взаимодействовать с реальными онлайн ничего не подозревающих пользователей; с помощью социальной инженерии техника для таргетинга; маршрутизации потоков данных или запуска распределенных атак типа отказа в обслуживании (DDoS-атаки) в целях пресечения информации. В случае

военных операций также физическое уничтожение или захват инфраструктуры информационно-коммуникационных технологий (ИКТ) является мощным способом повлиять на общественные дебаты.

Киберпреступники всегда начеку и ищут жертв с целью получения прибыли. Иногда они просто используют уязвимости программ, которые у нас есть на наших компьютерах. Другие, однако, готовят атаки вредоносных программ, используя новейшие и самые современные методы. Они делают это не из любви к искусству, они стремятся сделать свою работу прибыльной и увеличить свое личное достояние. Целью этих киберпреступников является кража данных для получения экономической прибыли. [1,с.76]

Уже в начале марта специализированная компания Check Point действительно установила, что было создано более 4000 веб-сайтов, связанных с новым коронавирусом. По ее словам, 3 процента из них служили злонамеренным целям, а 5 процентов были бы «подозрительными». Эти сайты могут использоваться для фишинговых целей, метод, который заключается в вымогательстве личной информации (пароля, кода банковской карты), выдавая себя за законный сайт.

Например, Check Point выявила фишинговую кампанию по электронной почте, направленную на очень большое количество итальянских получателей. В своих сообщениях хакеры объясняли, что «из-за большого количества коронавирусных инфекций в этом районе» ВОЗ предоставила документ, в котором перечислены меры предосторожности, которые необходимо предпринять для их предотвращения. Сообщение, хотя и подписанное врачом ВОЗ, конечно, не было получено от организации здравоохранения, и приложение было заражено.

Другие фишинговые электронные письма выдавались за Центры США по контролю и профилактике заболеваний в надежде обмануть получателей, в то время как власти Канады и Швейцарии также предупреждали о волне

вредоносных сайтов, использующих covid-19, выдавая себя за органы здравоохранения. [3,с.59]

В ответ ВОЗ справедливо предупредила, что «преступники «пытаются выдать себя за нее, чтобы» украсть средства или конфиденциальную информацию», и напомнила, что организация никогда не запрашивала пароль или имя пользователя или не отправляла нежелательные вложения.

Вредоносные электронные письма или веб-сайты могут также, помимо вымогательства информации или номеров банковских карт, использоваться для распространения вирусов, в том числе компьютерных. Несколько специализированных органов власти и компаний обнаружили, что эти электронные письма содержат, например, программное обеспечение для выкупа, вирусы, делающие данные компьютера недоступными и требующие выкупа за их разблокировку, или вредоносное ПО, предназначенное для восстановления учетных данных банковских счетов.

Согласно информации, на платформе отчетности полиции Pharos было зарегистрировано несколько вредоносных сообщений – в том числе электронные письма с подозрительными вложениями. Но на данный момент таких сообщений остается немного. [4,с.92]

Власти больше опасаются появления и распространения вводящей в заблуждение деловой практики, например, сайтов, которые продают маски, но никогда их не доставляют, или которые поставляют поддельный водно-охлаждающий гель. Власти сообщили о подозрительных объектах в Главное управление по вопросам конкуренции, потребления и борьбы с мошенничеством. Также следует опасаться призывов к мошенническим пожертвованиям, поскольку ВОЗ также предупредила об этом явлении.

В это время, когда французские больницы ожидают или сталкиваются с беспрецедентной рабочей нагрузкой, есть опасения, что компьютерная атака еще больше усложнит их деятельность.

Во Франции Anssi до сих пор не рассматривала ни одного крупного инцидента, связанного с covid-19. «Когда дело доходит до хакеров высокого уровня, мы ничего не наблюдаем, но мы начеку, чтобы избежать какого-то оппортунизма, и наши группы реагирования и обнаружения наблюдают за всем происходящим».

Однако современные средства защиты обладают ограниченными возможностями в прогнозировании кибератак или определении их источников. Бринт Милвард, ведущий исследователь гранта UA, говорит, что типичное понимание кибератак основано на изучении симптомов, а не болезни.[2,с.48]

В заключении хотелось бы отметить, что кибербезопасность имеет важное значение для защиты национальных интересов с точки зрения обороны и финансов, но эти потребности в области безопасности все чаще встречаются и в других секторах.

Список использованной литературы:

1. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А.И. Белоус, В.А. Солодуха – Вологда: Инфра-Инженерия, 2020г. – 692 с.

2. Белоус, А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: энциклопедия / А.И. Белоус, В.А. Солодуха – Москва: Техносфера, 2021г. – 482 с.

3. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд. – Москва: ДМК Пресс, 2017г – 434 с.

4. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя; перевод с английского Д.А. Беликова – Москва: ДМК Пресс, 2020г. – 326 с.

5. Международная безопасность: Глобальные и региональные акторы: коллективная монография / ответственные редакторы М.М. Лебедева, Ю.А. Никитина – Москва: Аспект Пресс, 2020г. – 320 с.