

УДК 004.056(73)

*А. А. Панас,
курсант 1-го курса факультета милиции
Могилевского института МВД
Научный руководитель: А. Е. Игнатович,
доцент кафедры
социально-гуманитарных дисциплин
Могилевского института МВД,
кандидат исторических наук*

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ПАНДЕМИИ COVID-19: ОПЫТ США

Киберпреступники используют Интернет в своих интересах. В условиях распространения COVID-19 кибербезопасность обрела свою специфику. Цель статьи — выявить особенности кибербезопасности в условиях пандемии на примере Соединенных Штатов Америки.

В разгар пандемии Министерство юстиции США процитировало «сообщения о физических и юридических лицах, продающих поддельные лекарства от COVID-19 в Интернете и участвующих в других формах мошенничества, сообщения от организаций, выдающих себя за Всемирную организацию здравоохранения или Центры по контролю и профилактике заболеваний, и сообщения о вредоносных программах, вставляемых в мобильные приложения, предназначенные для отслеживания распространения вируса», и другие сообщения, содержащиеся в докладе Управления ООН по наркотикам и преступности (UNODS) [1]. Правоохранительные органы отслеживают и расследуют такие киберинциденты.

Федеральное бюро расследований (далее — ФБР) и Национальная совместная рабочая группа по киберрасследованиям (NCIJTF) играют ведущую роль в реагировании на эти угрозы в США. Главные киберприоритеты ФБР включают борьбу с компьютерными и сетевыми вторжениями. Одна из ключевых проблем заключается в переходе от реагирования на вредоносные киберсобытия к предотвращению их. ФБР сосредоточило ресурсы на расследованиях компьютерных и сетевых вторжений, а также на расширении обмена информацией и координации с частным сектором. Национальная совместная рабочая группа по киберрасследованиям (NCIJTF) была создана в соответствии с Президентской директивой по национальной безопасности [2]. Миссия NCIJTF состоит в том, чтобы служить в качестве межведомственного национального координационного центра по координации, интеграции и обмену соответствующей информацией, связанной с расследованиями киберугроз. NCIJTF координирует

деятельность более 20 федеральных агентств, включая правоохранительные органы, разведку и вооруженные силы. NSIJTF также сотрудничает с частным сектором и международными партнерами. На раннем этапе были опасения, что NSIJTF не всегда делится информацией о киберугрозах между агентствами-партнерами. Были также высказаны критические замечания по поводу того, что NSIJTF воспринимается как расширение киберотдела ФБР вместо того, чтобы быть многоведомственной отдельной организацией. ФБР возглавляет несколько других целевых групп и партнерств, ориентированных на реагирование на киберугрозы. Например, в каждом отделении на местах имеются кибернетические целевые группы (CTFS). CTFS фокусируется на локальных угрозах кибербезопасности, реагирует на инциденты и поддерживает отношения с компаниями и учреждениями [2]. Кроме того, ФБР создало и поддерживает группы киберагентов и компьютерных ученых, которые могут быть быстро задействованы по всему миру для оказания помощи в расследовании компьютерных вторжений [2]. Они работают с правоохранительными органами в принимающих странах, чтобы поделиться информацией, сотрудничать в расследованиях и укреплять отношения с партнерскими агентствами. Эти сотрудники фокусируются на выявлении, устранении и ликвидации субъектов и организаций киберугроз.

Таким образом, особенностями обеспечения кибербезопасности в условиях пандемии в США являются: 1) активизация деятельности разветвленной структуры под руководством ФБР; 2) NSIJTF как межведомственный центр по координации, интеграции и обмену соответствующей информацией; 3) структура, которую дополняют кибернетические целевые группы и группы киберагентов по всему миру; 4) основные усилия структуры, которые направлены на расширение обмена информацией и координации с частным сектором.

1. Cybercrime and COVID19: Risks and Responses [Electronic resource]. URL: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf (date of access: 12.05.2021). [Перейти к источнику Вернуться к статье](#)

2. National Cyber Investigative Joint Task Force [Electronic resource]. URL: <https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force> (date of access: 12.05.2021). [Перейти к источнику Вернуться к статье](#)