УДК 385.81

# Компьютерный терроризм – новая форма терроризма XXI века. Стратегии противодействия кибертерроризму

Кондратюк Е.С.
Научный руководитель Блажко Д.В.
Белорусский национальный технический университет

**Введение.** В последнем десятилетии интенсивный технический прогресс и популяризация современных информационных технологий существенно повысили зависимость общества от информационных систем, надежность и функционирование информационных систем, инфраструктур, достоверность информации в открытых источниках и их защищенность. Появилась возможность использовать новые технологии в преступных и антисоциальных целях – это является главной антисоциальной проблемой современности. Сбои работы информационных систем отрицательно влияют на политические, экономические и общественные процессы, тем самым сея хаос в регионах, областях и даже в государствах. Сегодня террористические организации, используя спектр новых технологий, создают совершенно новые формы терроризма. Одной из таких форм является кибертерроризм (информационный терроризм).

**Основная часть.** Кибертерроризм (от англ. cyber – эпоха компьютеров) – предумышленное совершение действий, нарушающих функционирование компьютеров и/или телекоммуникационных сетей, либо угроза совершения таких действий, с намерением причинить вред или совершённая по социальным, идеологическим, религиозным или политическим мотивам; а также угроза личного характера, совершённая по тем же мотивам [1]. Данный термин был введен середине 1980-х годов сотрудниками американского института и разведки (ИБР). По их предположениям активное развитие данное явление получит в первых десятилетиях XXI века. Явление кибертерроризм тесно связано с понятием киберпреступность.

Киберпреступность (информационный криминал) – действие лиц или группы лиц, направленные на взлом, хищение или разрушение информационных систем в корыстных или хулиганских целях. Главным отличием кибертерроризма от информационного криминала является то, что киберпреступление, как правило, разовый акт, направленный против конкретного объекта киберпространства [2].

По мнению российского специалиста Е. Роговского, выделяется два вида кибертерроризма:

первый вид – это совершение террористических актов с помощью компьютеров и компьютерных сетей. Данное определение подразумевает со-

бой объединение «киберпространства» и «терроризма». И представляет собой умышленную атаку на объект киберпространства. К данному определению относятся правонарушения с использованием сети Интернет;

второй вид подразумевает собой непосредственное использование информационных пространств в следующих целях: повышение способностей террористических организаций, сбор информации для планирования террористических актов, агитационно-психологическое и информационно-психологическое воздействие на население и другая организационная деятельность.

Эффект кибертерроризма сравним с применением оружия массового поражения. Терроризм новой эпохи способен нарушать функционирование мировых экономических центров, деструктировать информационный обмен всего мирового общества.

По оценкам американских специалистов группа из десяти хакеров с сотней тысячью долларов способна затормозить поток информации на несколько недель. Двадцать хакеров с двумя сотнями тысяч долларов способны создать сбой в киберпространстве страны. Организация кибертеррористов с миллионом долларов способны полностью разрушить информационную систему таких государств как США, Россия, Канада, Китай и т.д.

Такие прогнозы вынудили американское правительство выделить значительные средства, около 25,2 млрд. долларов, на реализацию концепции «Отражение атак в информационной сфере» до 2016 года. До этого затраты на охрану киберпространства США выделяло около 18 млрд. долларов.

В 2010 году впервые было обнаружено первое в мире кибероружие – Stuxnet. Stuxnet – это первый в мире компьютерный червь, перехватывающий и модифицирующий информационный поток компьютеров под управлением операционных систем Windows [3]. Вирус был обнаружен 17 июня 2010 года белорусским экспертом «ВирусБлокАда» Сергеем Уласенем. Вирус был замечен как в компьютерах рядовых пользователей, так и промышленных системах. По неподтверждённой информации вирус является детищем американских и израильских специалистов и имеет сугубо политический аспект. Основной целью программы было приостановить иранскую ядерную программу на несколько лет. Вирус нарушил работу около 1 000 центрифуг, предназначенных для обогащения ядерного топлива. Правительству удалось избавиться от вируса после уничтожения более 1 000 устройств.

Эффективно противодействовать киберпреступности можно только объединив усилия. Поэтому в 2018 году был проведен Первый Международный конгресс по кибербезопасности, который состоялся в Москве

5–6 июня. В нем приняли участие представители 681 организаций из более чем 50 стран [2].

Ввиду опасности кибертерроризма мировое сообщество разработало ряд направлений противодействия кибертерроризму. К ним относятся:

1) развитие и укрепление сотрудничества между государствами и их специальными организациями в сфере обеспечения информационной безопасности (Интерпол, Организация экономического сотрудничества и развития, SWIFT ( Сообщество всемирных межбанковских финансовых каналов связи), ICANN (интернет-корпорация по присвоению имен и номеров));

2) обмен информацией о кибертеррористических угрозах между государствами;

3) привлечение лиц, задействованных в кибертерроризме, к уголовной ответственности;

4) разъяснение политики государства в информационном пространстве.

Для обеспечения безопасности в киберпространстве специалисты советуют:

1) удалить историю со скриншотами паролей от социальных сетей;

2) не переходить по неизвестным ссылкам;

3) подключить для всех социальных сетей двухфакторную аунтефикацию;

4) пользуйтесь приложениями, а не сайтами;

5) не пересылайте фото своих банковских карточек;

6) при подключении к Wi-Fi общего пользования используйте специальные приложения типа Kaspersky Secure Connection;

7) не используйте один и тот же пароль.

**Заключение.** Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека возрастает вероятность использование технических средств в различных преступных направлениях. Чем сильнее становиться зависимость жизни общества от компьютерных сетей, тем опаснее уязвимость общества от всевозможных атака кибертеррористов.

**Литература**

1. Информационный терроризм: выработка стратегии противодействия [Электронный ресурс]. – 2021. – Режим доступа: http://ecsocman.hse.ru/data/2014/01/16/1251303793/Turonok.pdf – Дата доступа: 09.04.2021.

2. КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ВИДЫ И СПОСОБЫ БОРЬБЫ С НЕЙ [Электронный ресурс]. – 2021. – Режим доступа https://kubsu.ru/sites/default/files/users/21554/portfolio/kursach_1_0.pdf – Дата доступа: 09.04.2021.

3. Stuxnet [Электронный ресурс]. – 2021. – Режим доступа: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html – Дата доступа: 08.02.2017.

УДК 385.81

## Бітва за Маскву

Кандрацюк Я. С.
Навуковы кіраўнік Савік С. А.
Беларускі нацыянальны тэхнічны універсітэт

**Уводзіны.** Маскоўская бітва, гэтак жа вядомая, як аперацыя «Тайфун», з'яўляецца самай вялічнай не толькі ў Другой сусветнай вайне, але і ва ўсёй вайсковай гісторыі чалавецтва. З захопам Масквы, ключавога пункта ўсходняй кампаніі 1941 г., паводле планаў Вермахта, Савецкі Саюз павінен быў страціць сваю дзяржаўнасць. Утрыманне сталіцы давала магчымасць Савецкаму камандаванню атрымаць патрэбны час для разгортвання ў поўным маштабе вайсковай эканомікі, мабілізацыі ўсіх рэсурсаў. Маскоўская бітва ўяўляла сабою сукупнасць абарончых і наступальных аперацый савецкіх войскаў, праведзеных з 30 верасня 1941 г. па 20 красавіка 1942 г.

**Асноўная частка.** Аперацыя «Тайфун» пачалася 30 верасня 1941 года. «Тайфун» – наступальная аперацыя нямецка-фашысцкіх войскаў у верасні – лістападзе 1941 г., асноўнай цэллю аперацыі быў захоп Масквы і Маскоўскага прамысловага раёна. [1] Аперацыя «Тайфун» рыхтавалася ў той момант, калі ў Чырвонай Арміі склалася цяжкае становішча, бо на шэрагу накіраванняў суперніку атрымалася дамагчыся значных поспехаў. У адпаведнасці з задумай аперацыі меркавалася стварыць на флангах групы войска «Цэнтр» моцныя танкавыя часткі і ў выніку падвойнага ахопу атачыць горад Вязьма. 5 і 6 кастрычніка 1941 года немцам атрымалася атачыць 5 савецкіх войскаў, колькасцю больш за 600 тысяч чалавек, так званы «Вяземскі кацёл». Аднак аточаныя войскі аказвалі значны супраціў, які ўскладніла пасоўванне нямецкіх войскаў, было скавана каля 20 нямецкіх дывізій. Ужо на пачатак аперацыі камандаванне войска «Цэнтр» здолела атрымаць верагодныя звесткі пра месцаванне савецкіх войскаў. Хібныя дадзеныя нямецкай выведкі не паўплывалі на вынікі пачатковага этапу, але