МОНИТОРИНГ температуры совести

Фундаментальные структурные изменения, связанные с пандемией коронавирусной инфекции COVID-19, одномоментно затронули все сферы общественной и личной жизни людей. Конечный результат перемен в социальных и экономических системах пока не совсем понятен и постоянно обсуждается на различных форумах. Но уже очевидно, что роль информационно-коммуникационных технологий в дальнейшем развитии общества будет определяющей. При этом рост уровня информатизации предполагает явную необходимость усиления информационной безопасности (ИБ).

Обзор условий обеспечения информационной безопасности в период COVID-19 «Весніку сувязі» представляет к. т. н., доцент УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь Владимир Викторович МАЛИКОВ.

В основе базовых технологических моделей для всех сегментов коммуникации будут находиться: устройства (ЭВМ/ЭВС), программное обеспечение (операционные системы / прикладное ПО), каналы сопряжения и коммуникации (радиоканал / выделенные физические линии / ВОЛС).

При реализации вариантов коммуникации пользователю/предприятию необходимо принять один из вариантов стратегии использования устройств, который включает определенный набор правовых/технологических аспектов ИБ [2]:

1. BYOD (Bring Your Own Device, «принеси свое устройство»): использование собственных персональных устройств в личных и рабочих целях.

2. CYOD (Choose Your Own Device, «выбери свое устройство»): предприятие предоставляет возможность своим сотрудникам выбрать устройства из определенного списка. В этом случае компания покупает и несет ответственность за управление устройствами, контроль над обновлениями и установками приложений.

3. COPE (Corporate-Owned, Personally Enabled, «корпоративные устройства, настройкой и обслуживанием которых сотрудник занимается самостоятельно»): предприятие предоставляет сотруднику устройство с разрешением на использование этого устройства в личных и рабочих целях.

4. COBO (Company Owned / Business Only, «принадлежит компании / только бизнес») – мобильные устройства, принадлежащие компании, предназначенные только для профессионального использования и полностью управляемые компанией.

5. COSU (Company Owned / Single Use, «принадлежит компании / специфического использования») – выделенные устройства, принадлежат компании, и их доступ ограничен для одного или очень специфического использования (терминалы/киоски).

Для организации любых видов удаленной работы по каналам сопряжения и коммуникации (радиоканал / выделенные физические линии /ВОЛС), в том числе обеспечения вопросов ИБ, осведомленные пользователи используют технологии VPN (Virtual Private Network, «виртуальная частная сеть») [3].

Согласно статистике мировой спрос на использование VPN в марте 2020 года вырос на 41% и остается на 22 % выше, чем до начала пандемии. Самый высокий объем спроса на VPN: США (+41 %), Великобритания (+35 %) и Франция (+80 %) [4].

Основные сегменты социальных и экономических систем общества, подвергаемых интенсивной трансформации и требующих усиления контроля в вопросах ИБ: досуг/общение, системы мониторинга и контроля самоизоляции дистанционная работа/образование, онлайн-покупки/платежи.

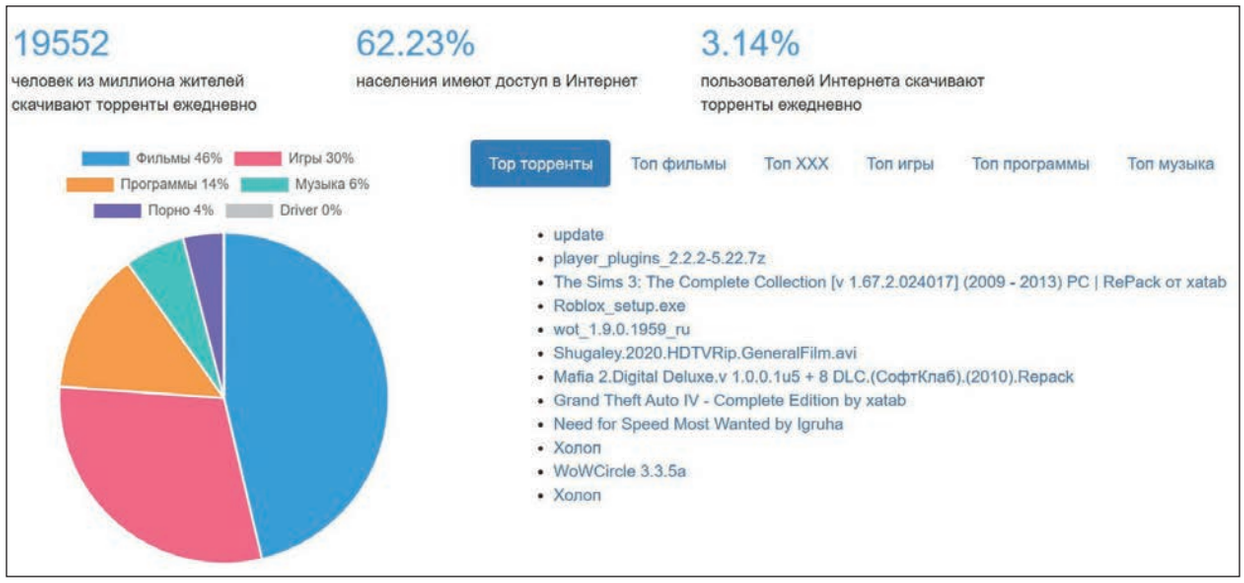


Рисунок 1 – Статистика в BitTorrent-сети в Беларуси за 05.05.2020 [5]

Досуг/общение

В период вынужденной самоизоляции возможности досуга и общения сводятся преимущественно к развлекательному контенту и социальным сетям / мессенджерам.

Более 3 % белорусских пользователей сети интернет ежедневно пользуются торрент-сервисами [5] (рис. 1), которые, как правило, распространяют пиратский мультимедийный контент (фильмы, игры) и нелицензионное ПО (Adobe Photoshop, Microsoft Office, Sony Vegas Pro и др.), в состав которого киберпреступники внедряют различные уязвимости/закладки.

Среди социальных медиа наблюдается рост Facebook, YouTube [6] (рис. 2).

Следует отметить, что белорусы в основном используют мобильные устройства китайских/корейских производителей Xiaomi, Samsung, Huawei [6] (рис. 3) с мобильной операционной системой Android (84,75 %). При этом только около 17 % пользователей используют ее последнюю версию семейства 10.0, включающую самые новые обновления безопасности (рис. 4).

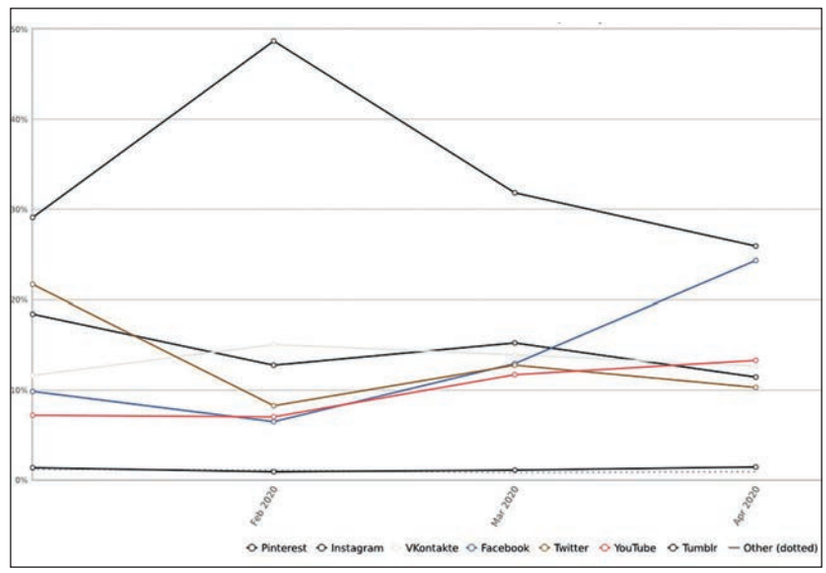


Рисунок 2 – Статистика использования социальных медиа в Беларуси (январь–апрель 2020)[6]

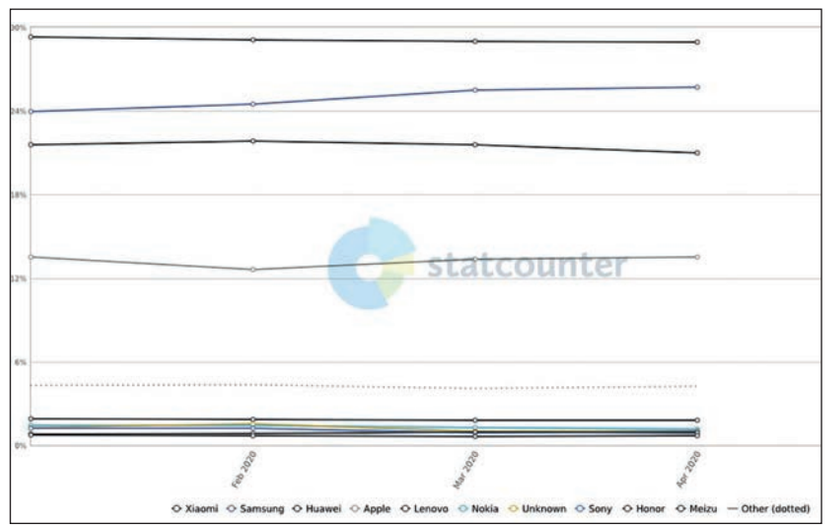


Рисунок 3 – Статистика использования мобильных устройств Беларуси (январь–апрель 2020) [6]

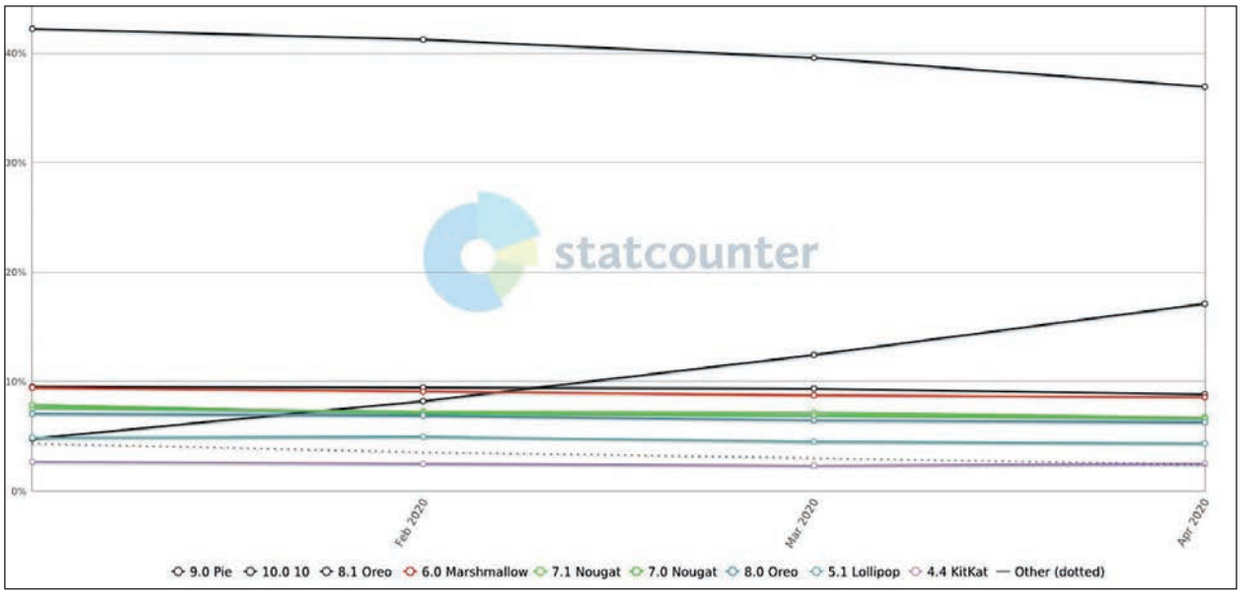


Рисунок 4 – Статистика используемых версий мобильной ОС Android в Беларуси (январь–апрель 2020) [6]

Системы мониторинга и контроля самоизоляции COVID-19

В эпоху пандемии большинство стран мира пошли на усиленные меры организации контроля населения на основе специального ПО, устанавливаемого на мобильные устройства.

Согласно отчетным данным [4], для контроля распространения COVID-19 используются:

приложения отслеживания контактов – 29 стран;

альтернативные меры цифрового отслеживания – 30 стран;

технологии физического наблюдения – 9 стран;

цензура, связанная с COVID-19, была введена 15 странами.

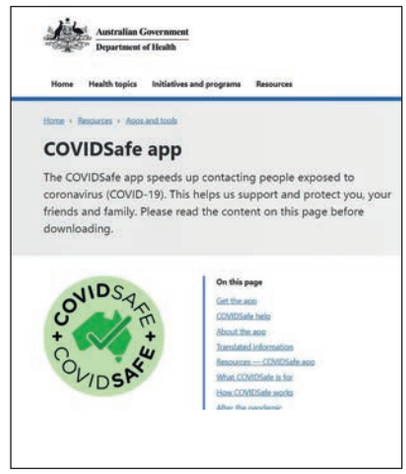
В настоящее время в мире доступно 53 приложения для отслеживания контактов (рис. 5):

Aarogya Setu Mobile App (Индия) [9] является самым популярным (более 50 млн загрузок);

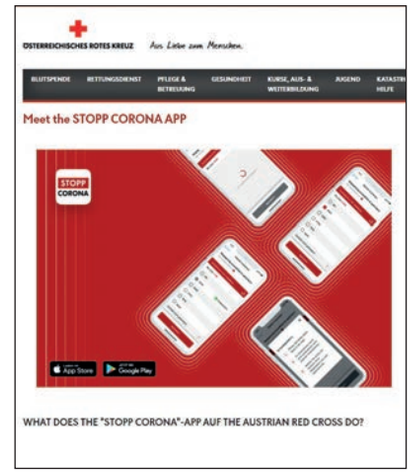
25 % приложений не имеют политики конфиденциальности;

57 % используют GPS, 15 % используют Bluetooth и 26 % используют GPS и Bluetooth.

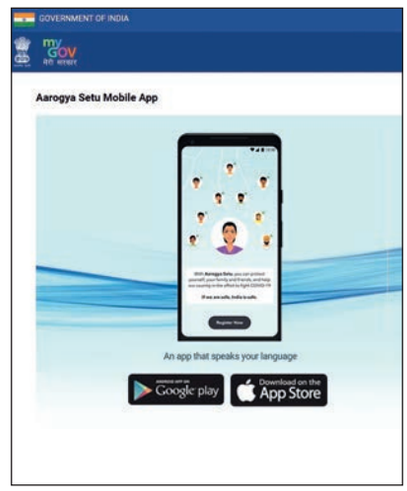
При этом детального исследования указанных выше приложений по вопросам ИБ не проводилось.



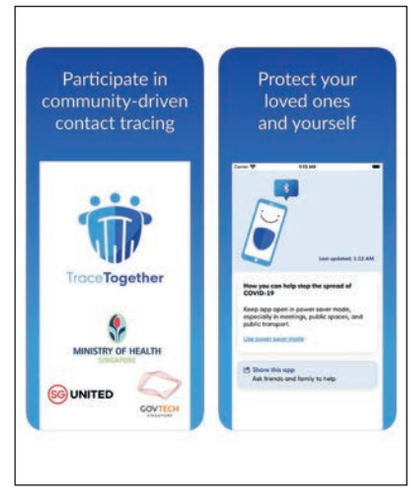
а) Австралия (более 500 тыс. загрузок) [7]



б) Австрия (более 100 тыс. загрузок) [8]



в) Индия (более 50 млн загрузок) [9]



г) Сингапур (более 50 тыс. загрузок) [10]

Рисунок 5 – Приложения государственных органов для отслеживания контактов COVID-19

Дополнительно в нашей жизни возникли системы дистанционного мониторинга температуры персонала/посетителей (таблички «Внимание! Ведется тепловизионный контроль»). Такие системы на основе оборудования Hikvision (видеокамеры DS-2TD2637B-10/P) уже установлены на станциях метрополитена и железнодорожного вокзала г. Минска (рис. 6).

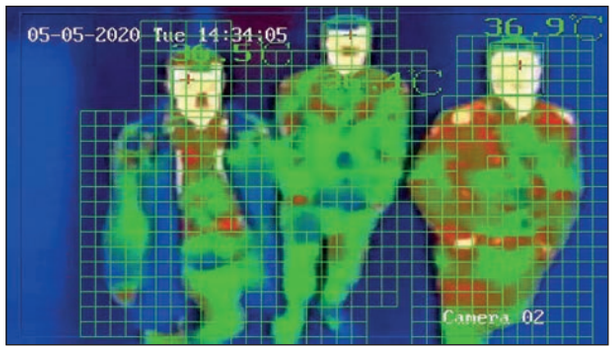
Система позволяет выявлять людей с повышенной температурой в потоке и принимать соответствующие меры согласно инструкции. В данном случае необходимо проведение дополнительного нормативно-правового регулирования, включая вопросы соблюдения ИБ, при эксплуатации таких систем со стороны организаций/предприятий.

а)

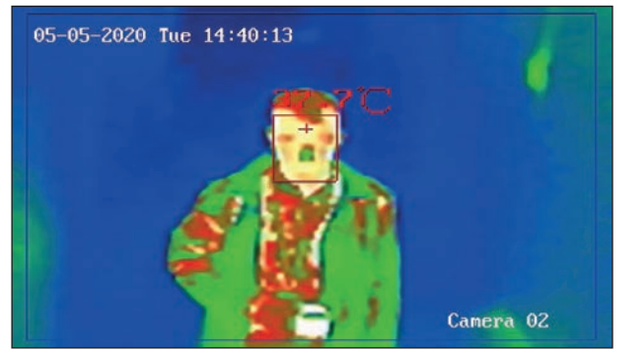
б)

в)

г)



д)



е)

Рисунок 6 – Системы дистанционного мониторинга температуры персонала/посетителей

Образование / дистанционная работа

Агентство Национальной Безопасности (АНБ) США опубликовало краткое руководство по выбору сервиса для теле- и web-конференций [11].

В качестве основных параметров оценки были предложены:

реализация сквозного шифрования;

использование надежных, хорошо известных и проверяемых стандартов шифрования;

использование многофакторной аутентификации для проверки личности пользователей;

возможность контроля за подключением к сеансам конференций;

возможность предоставления данных третьим сторонам согласно политике конфиденциальности;

возможность безопасного удаления данных из сервиса и его репозиториев пользователями в случае необходимости;

проверка или сертификация сервиса государственным органом, занимающимся вопросами безопасности;

оценка облачных сервисов в рамках программы FEDRAMP Административно-бюджетного управления США.

По результатам исследования 13 популярных сервисов для теле- и web-конференций установлено, что ни один из них не соответствует предъявленным требованиям по вопросам ИБ полностью [11].

Онлайн-покупки/ платежи

По данным Федеральной торговой комиссии США (FTC) [12] (рис. 7), обобщившей жалобы пострадавших, в период с 01.01.2020 по 05.05.2020 из-за мошенничеств, связанных с COVID-19, уже было потеряно более 24,44 млн долларов США.

Вывод

Дальнейшие изменения, связанные с пандемией коронавирусной инфекции COVID-19, потребуют от пользователей/организаций усиления нормативно-правового, организационно-технического и технического обеспечения мер ИБ при организации любых видов удаленной работы по каналам сопряжения и коммуникации.

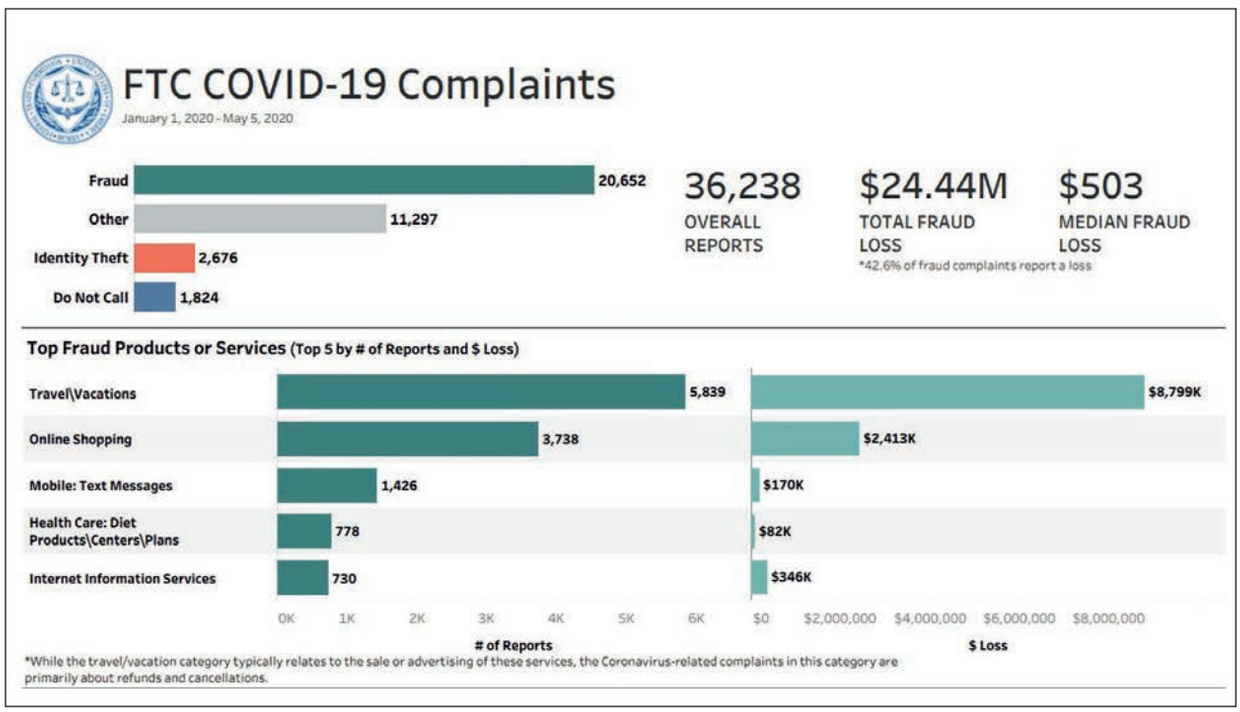


Рисунок 7 – Статистика FTC по мошенничествам, связанным с COVID-19 [12]

ЛИТЕРАТУРА

1. The Coronavirus Outbreak // nytimes.com [Электрон. ресурс]. – 2020. – Режим доступа: https://www.nytimes.com/news-event/coronavirus?smid=fb-share&fbclid=IwAR2 K4SsVo89MRh9uda0lPZSUVOnpjQT99lqLlY6CZphUCEl44MfF_vkrStE. – Дата доступа: 05.05.2020.
2. BYOD, CYOD, COPE, COBO, COSU. A wide range of devices ownership & usage // tinymdm.net [Электрон. ресурс]. – 2020. – Режим доступа: https://www.tinymdm.net/byod-cyod-cope-cobo-cosu/. – Дата доступа: 05.05.2020.
3. The Ultimate VPN Guide for Newbies in May 2020: What's a VPN? Do You Need One? // vpnmentor.com[Электрон. ресурс]. – 2020. – Режим доступа: https://www.vpnmentor.com/blog/vpns-101-vpnmentors-vpn-guide-newbies/. – Дата доступа: 05.05.2020.
4. Research // top10vpn.com [Электрон. ресурс]. – 2016-2020. – Режим доступа: https://www.top10vpn.com/research/. – Дата доступа: 06.05.2020.
5. Статистика в BitTorrent-сети // iknowwhatyoudownload.com [Электрон. ресурс]. – 2020. – Режим доступа: https://iknowwhatyoudownload.com/ru/stat/BY/daily. – Дата доступа: 05.05.2020.
6. Statcounter // statcounter.com [Электрон. ресурс]. – 2020. – Режим доступа: https://gs.statcounter.com/. – Дата доступа: 06.05.2020.
7. COVID Safe app // health.gov.au [Электрон. ресурс]. – 2020. – Режим доступа: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app. – Дата доступа: 06.05.2020.
8. Meet the STOPPCORONAAPP // roteskreuz.at [Электрон. ресурс]. – 2020. – Режим доступа: https://www.roteskreuz.at/site/meet-the-stopp-corona-app/. – Дата доступа: 06.05.2020.
9. Aarogya Setu Mobile App // mygov.in [Электрон. ресурс]. – 2020. – Режим доступа: https://www.mygov.in/aarogya-setu-app/. – Дата доступа: 07.05.2020.
10. Responding to COVID-19 with Tech // tech.gov.sg [Электрон. ресурс]. – 2020. – Режим доступа: https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/. – Дата доступа: 07.05.2020.
11. Selecting and Safely Using Collaboration Services for Telework // defense.gov [Электрон. ресурс]. – 2020. – Режим доступа: https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF?fbclid=IwAR2vOQr-_nFdGNVwceLRNOXn5NygddJMJ-mK9r79_WfZhGUXteX2YSwJhZQ.– Дата доступа: 07.05.2020.
12. FTCCOVID-19 // www.ftc.gov [Электрон. ресурс]. – 2020. – Режим доступа: https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints.pdf. – Дата доступа: 07.05.2020.