



Защита национального информационного пространства в новых реалиях 2020-2021 гг.

Москва. 27 апреля 2021 г.



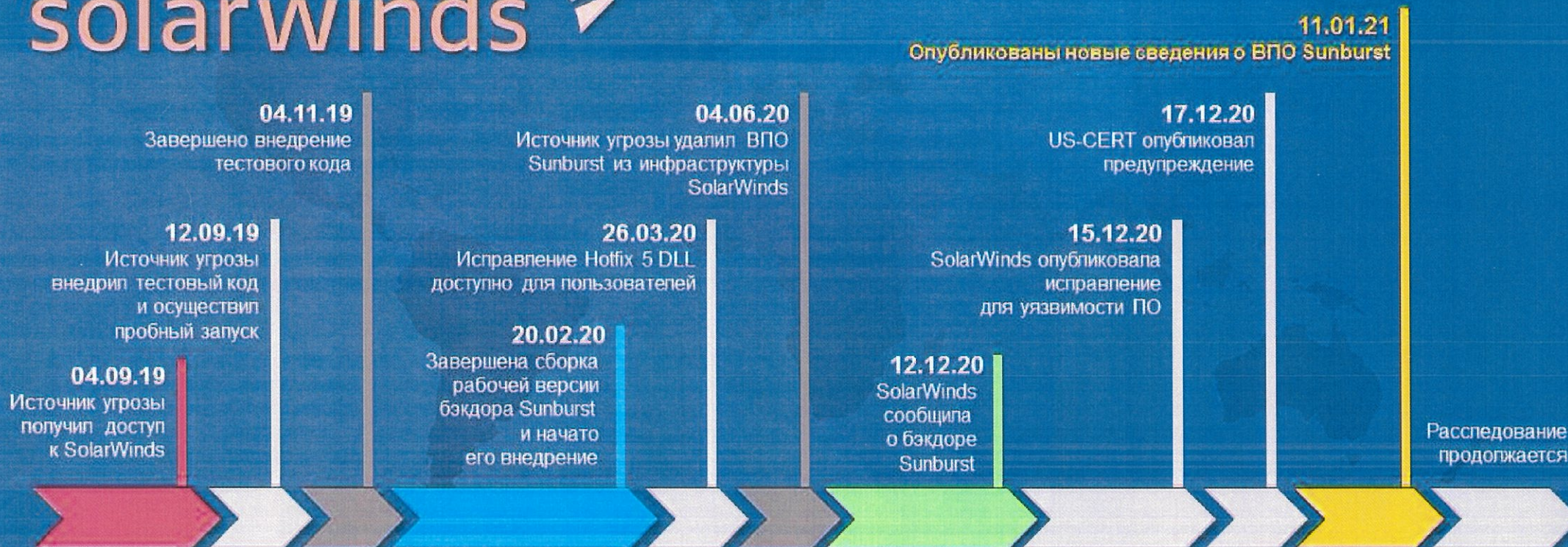
Пресечение функционирования вредоносных ресурсов

2





Взлом ПО компании SolarWinds





Монополизация рынка ИКТ





Проблемы унификации цифровой среды

EXPLOIT

Database

Currently Archiving
9468
Exploits

[home] [remote] [local] [web] [dos] [search] [archive] [submit] [rss]

The Exploit Database

16th Nov 2009:

The ultimate archive of exploits and vulnerable software and a great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy to navigate database. When possible, we've added the vulnerable software for download. We are still in the process of organizing the database. You can Download the relevant exploit by clicking the "D" and when available, download the Vulnerable Application using the "A" link."

Remote Exploits

Date	D	A	Description	Plat.	Author
2009-11-16	D	-	Novell eDirectory 8.8 SP5 iConsole Buffer Overflow	windows	Matteo Memelli
2009-11-16	D	-	HP Power Manager Administration Universal Buffer Overflow Exploit	windows	Matteo Memelli
2009-11-13	D	-	Samba 3.0.10 - 3.3.5 Format String And Security Bypass Vulnerabilities	multiple	Jeremy Allison
2009-11-13	D	-	PHP 5.2.11/5.3.0 Multiple Vulnerabilities	php	Maksymilian Arciemowicz
2009-11-12	D	A	EasyMail Objects EMSMTP.DLL 6.0.1 ActiveX Control Remote Buffer Overflow Vulnerability	windows	Will Dormann
2009-11-12	D	-	WebKit 'Document()' Function Remote Information Disclosure Vulnerability	multiple	Chris Evans
2009-11-12	D	-	WebKit XML External Entity Information Disclosure Vulnerability	multiple	Chris Evans



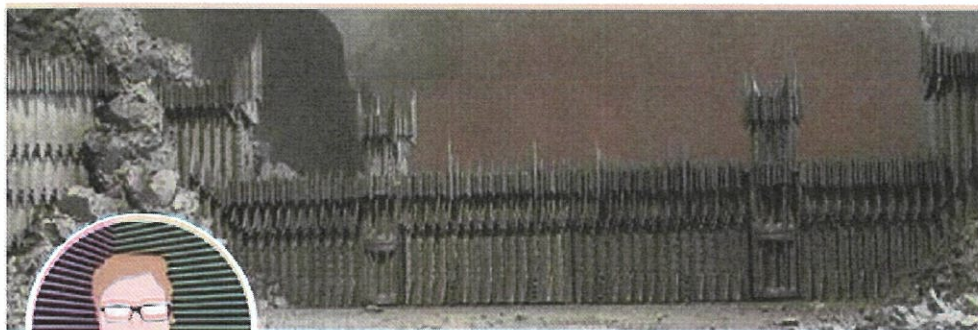


Расследование инцидента с SolarWinds



Ian Thornton-Trump CD

21,6 тыс. твит



Читать

Ian Thornton-Trump CD

@phat_hobbit

Еще в 2017 году предупреждал о существовавших проблемах с обеспечением кибербезопасности

2 022 в читаемых 13,2 тыс. читатель

Твиты

Твиты и ответы

Медиа

Нравится



Твитнуть



Zack Whittaker @zackwhittaker · 15 дек. 2020 г.

SolarWinds, whose software was backdoored to allow hackers to breach U.S. government agencies, was warned last year that anyone could access its update server using the password "solarwinds123" per [@bing_chris](#) and [@trazrael](#).



Пароль доступа к серверу обновления был примитивным - «solarwinds123», и подобрать его мог любой атакующий



Hackers used SolarWinds' dominance against it in sprawling spy camp... On an earnings call two months ago, SolarWinds Chief Executive Kevin Thompson touted how far the company had gone during his 11 years... [@reuters.com](#)

402

4,2 тыс.

5,7 тыс.





Повышение осведомлённости пользователей об актуальных угрозах



Портал «Безопасность пользователей
в сети Интернет»

<http://www.safe-surf.ru>

Медиа об информационной безопасности

Как не стать жертвой фишинга на работе

**КАК НЕ СТАТЬ ЖЕРТВОЙ
ФИШИНГА НА РАБОТЕ**

Фишинговая рассылка – первый этап любой компьютерной атаки на компанию

Согласно выводам аналитиков,
4 из 10 сотрудников
обследованных организаций
открывают фишинговые письма




Медиа об информационной безопасности

Соблюдайте цифровую гигиену!

**Соблюдайте
цифровую гигиену!**

ЧИСТОТА УСТРОЙСТВА



- Регулярное обновление ОС и ПО
- Парковка личных данных только на защищённых каналах
- Регулярное резервное копирование
- Полное удаление файлов с устройств



Информирование об угрозах безопасности и рекомендациях по их нейтрализации

8



Портал «Безопасность пользователей
в сети Интернет»

<http://www.safe-surf.ru>

НКЦКИ

Федеральный информационный центр
по безопасности информации
www.fkie.ru
8 800 707 08 08

Об угрозах безопасности информации, связанных с пандемией
коронавируса (COVID-19).

ALRT-20200320.1 | 30 марта 2020 г.
1-й выпуск

Информация об угрозах безопасности информации

Пользователи в сети Интернет сталкиваются с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19). В настоящее время пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19).

Следует учитывать, что пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19). В настоящее время пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19).

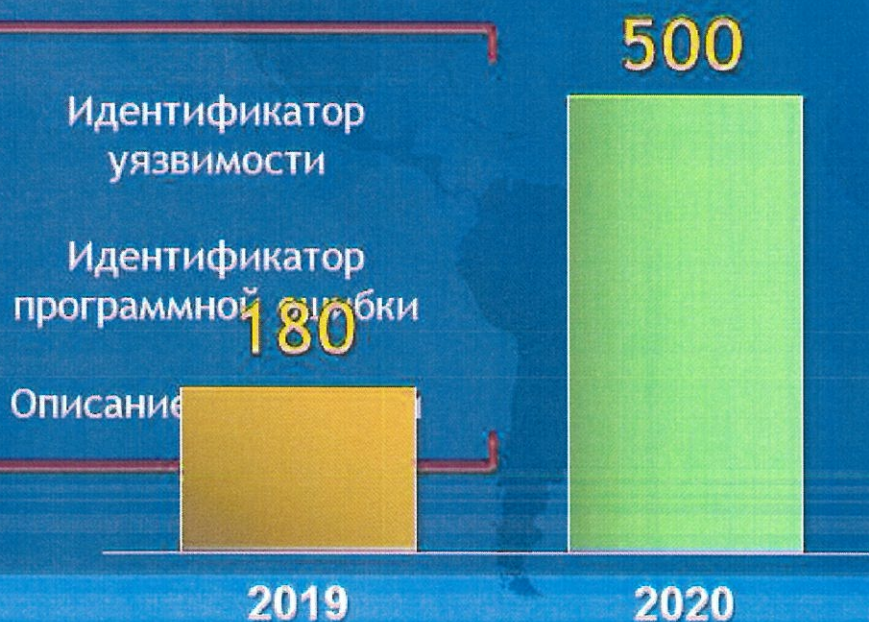
Пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19). В настоящее время пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19).

Пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19). В настоящее время пользователи могут столкнуться с угрозами безопасности информации, связанной с пандемией коронавируса (COVID-19).



Информирование об актуальных уязвимостях ПО и угрозах безопасности

Направлено информационных бюллетеней



НКЦКИ

Национальный координационный центр по компьютерным инцидентам
Веб сайт: ncc.ki.gov.ru
E-mail: threat@ncc.ki.gov.ru

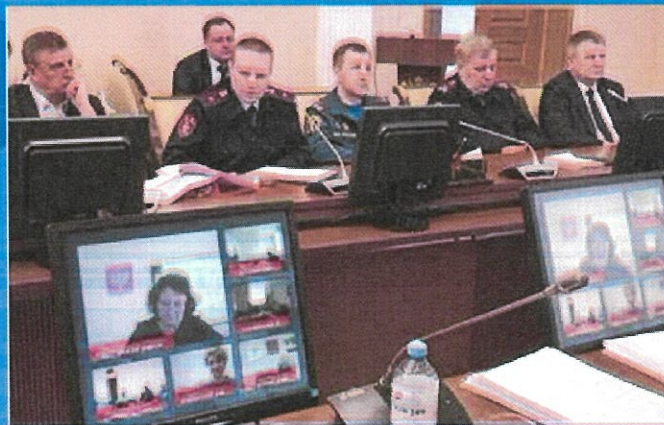
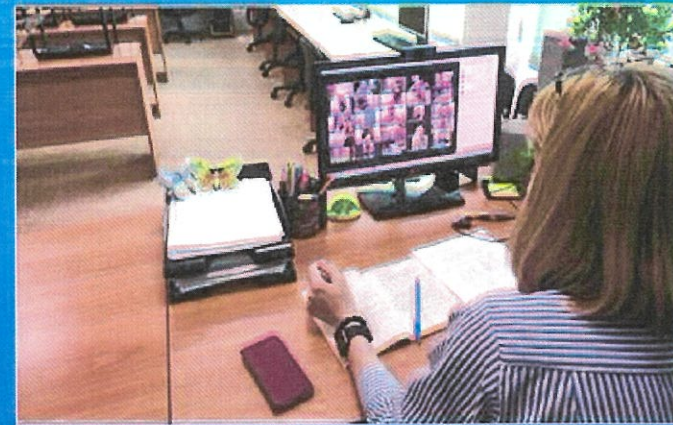
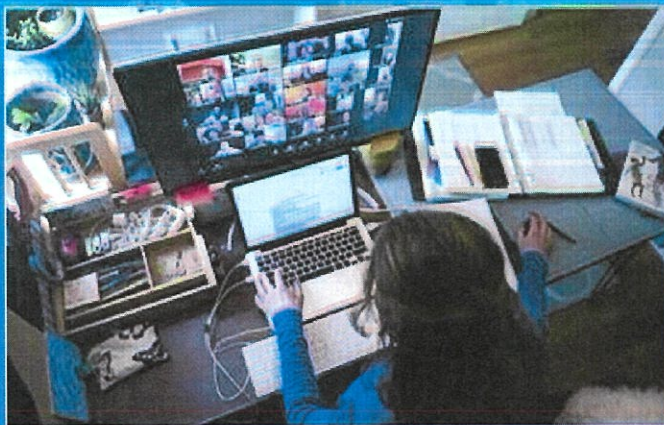
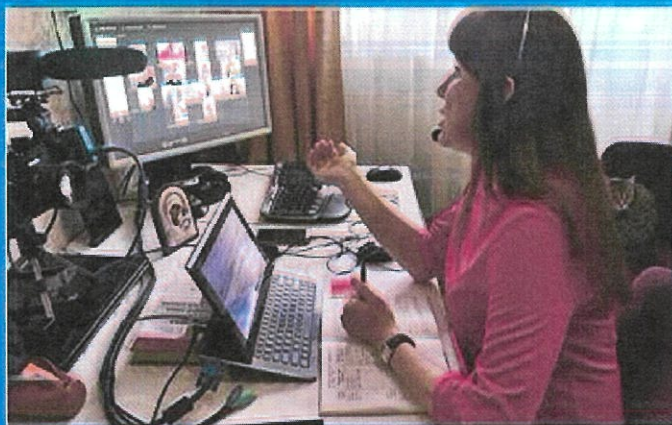
Уведомление об уязвимости
УИД: 20210322 в 10 марта 2021 г.
Уровень опасности: **КРИТИЧЕСКИЙ**
Направление обновления: **ЕСТЬ**

Выполнение произвольных команд оболочки в Creative Cloud Desktop Application

Идентификатор уязвимости	MITRE: CVE-2021-21078
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Creative Cloud Desktop Application 5.1.0.407, 5.2.0.436, 5.2.1.441, 5.3.1.470, 5.3.5.499, 5.3.5.518
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 марта 2021 г.
Дата обновления	10 марта 2021 г.
Оценка критичности уязвимости (CVSS v3.1)	9.8 AU/IAE U/RB N/D/+/S U/E N/A/N/A
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (P)

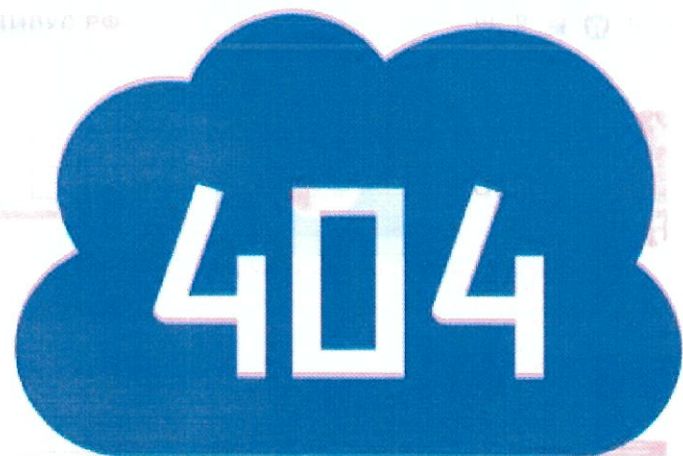


Изменение обстановки в информационном пространстве





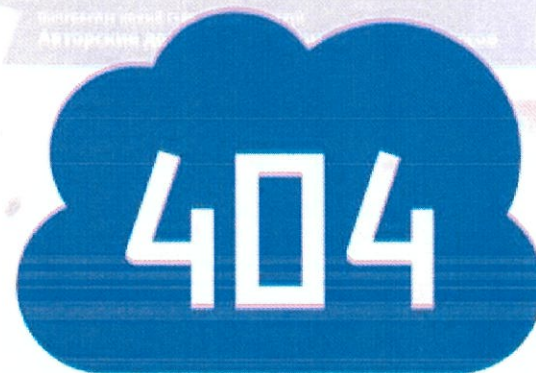
Единичные факты недоступности информационных систем общего пользования



Page not found



Page not found

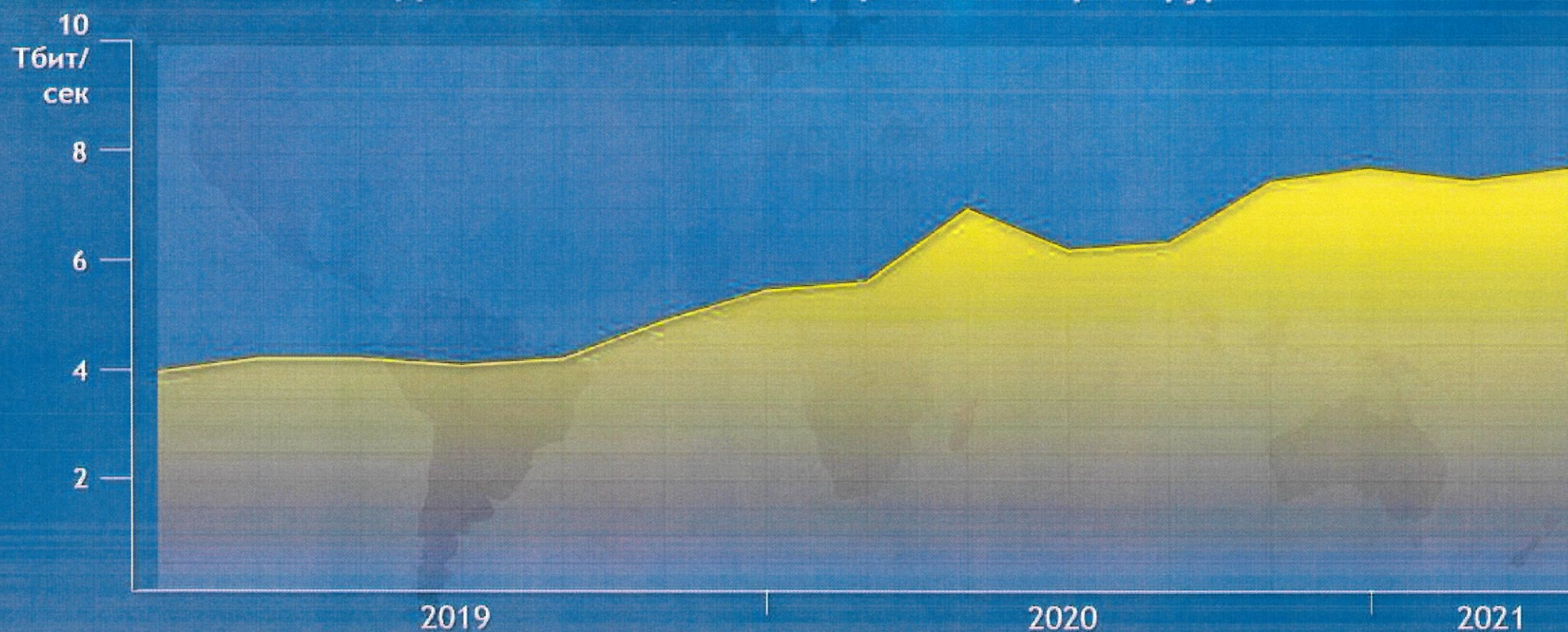


Page not found



Объем глобального трафика сети Интернет

Данные точки обмена трафиком в г. Франкфурт



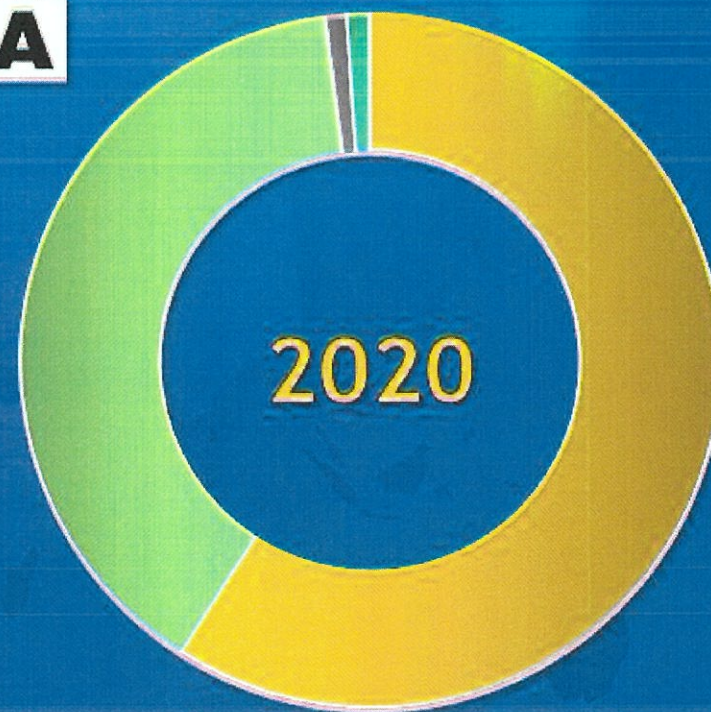
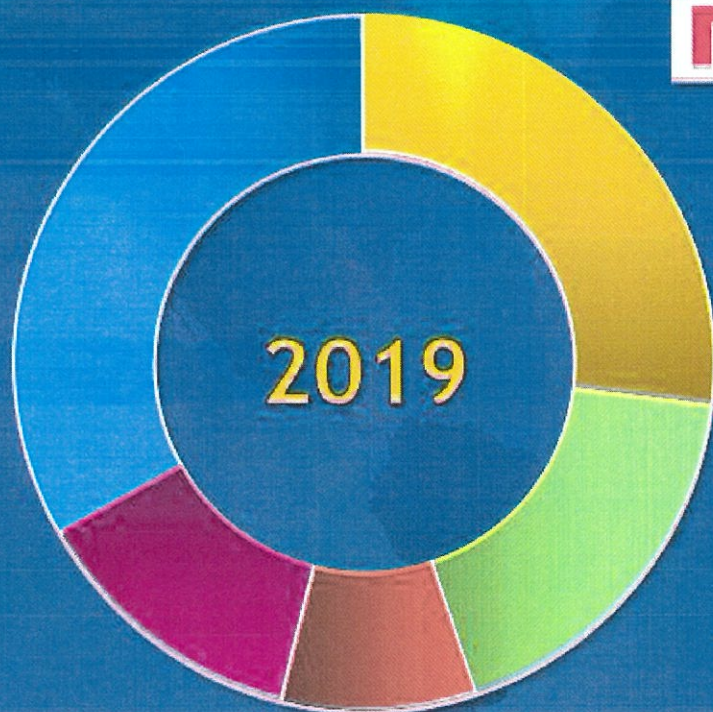
■ среднее значение трафика







Источник: DE-CIX Management GmbH



Основные цели компьютерных атак

ГОССОПКА



- | | | |
|--|--|---|
|  органы государственной власти |  предприятия промышленности |  наука и образование |
|  кредитно-финансовая сфера |  объекты здравоохранения |  энергетика |
| | |  прочее |



Примеры компьютерных атак методом социальной инженерии



От: Новейшая клиника
по борьбе с COVID-19



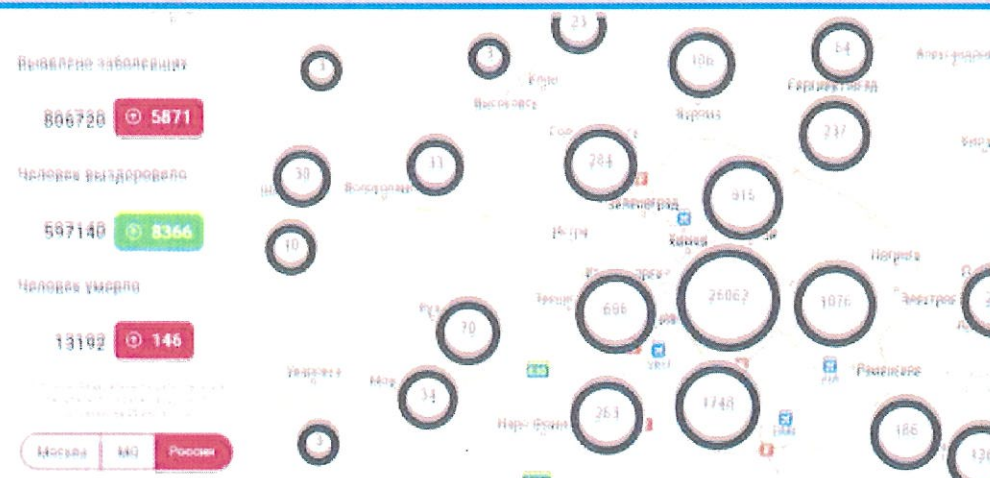
Клиника проводит беспрецедентную
акцию!!! Бесплатная сдача анализов
на антитела к COVID-19

Заполните форму
записи к врачу



Онлайн карта
распространения COVID-19

Поиск по карте




Для постоянного доступа к карте
скачайте мобильную версию








Примеры компьютерных атак методом социальной инженерии

**Бесплатные консультации
больным COVID-19**

Поиск






Для получения консультации
перейдите по ссылке




8-800-800-800



Covid19@bk.net





**Помощь в получении
цифрового пропуска**




Поиск





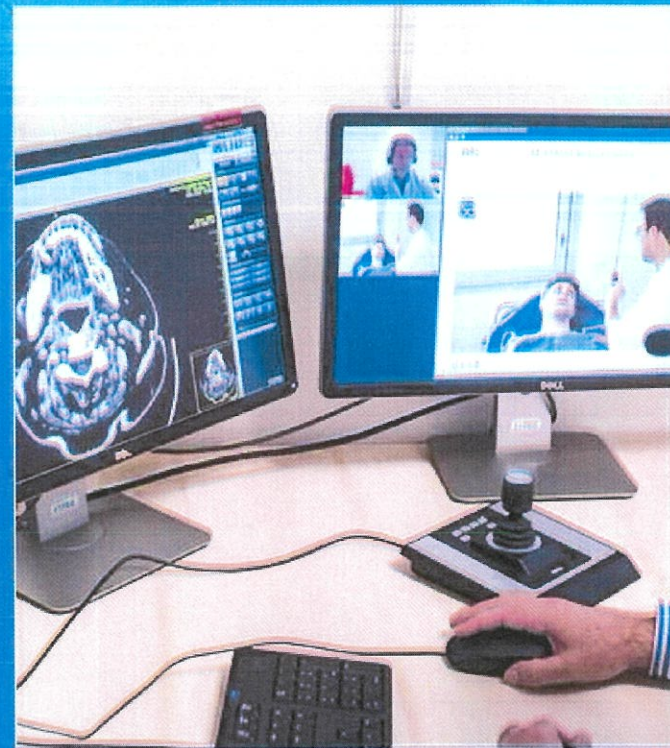
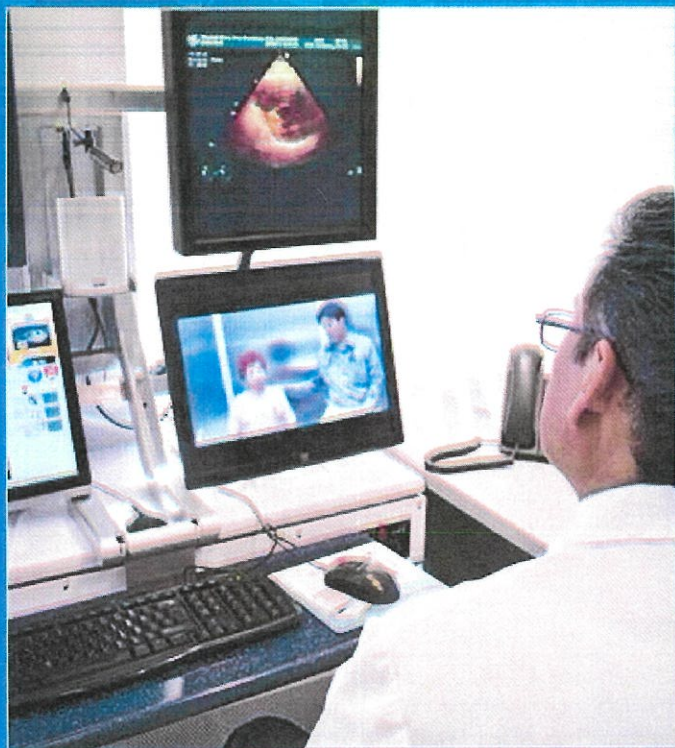
Заполните форму
и перейдите по ссылке







Нарушение конфиденциальности в системах телемедицины



Новый объект компьютерных атак: системы телемедицины



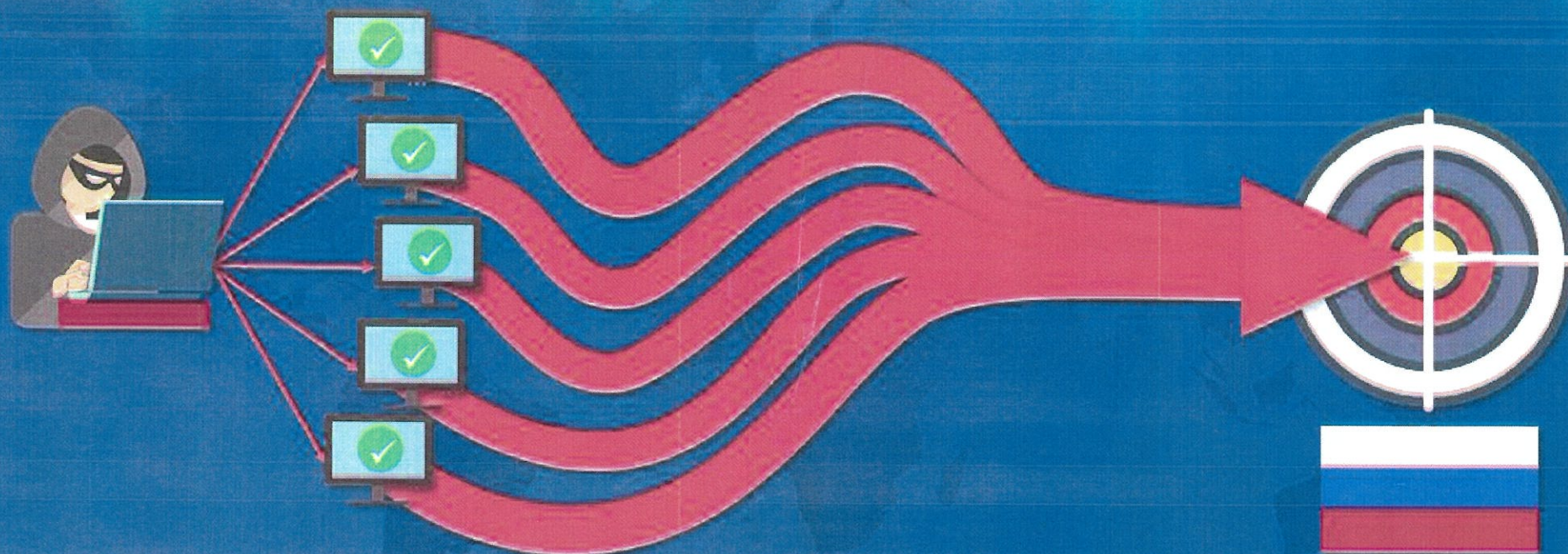
Компьютерные атаки на информационные ресурсы ФБУН ГНЦ ВБ «Вектор»

Внедрение вредоносного программного обеспечения





2020: увеличение крупномасштабных DDoS-атак на российские информационные ресурсы



2020

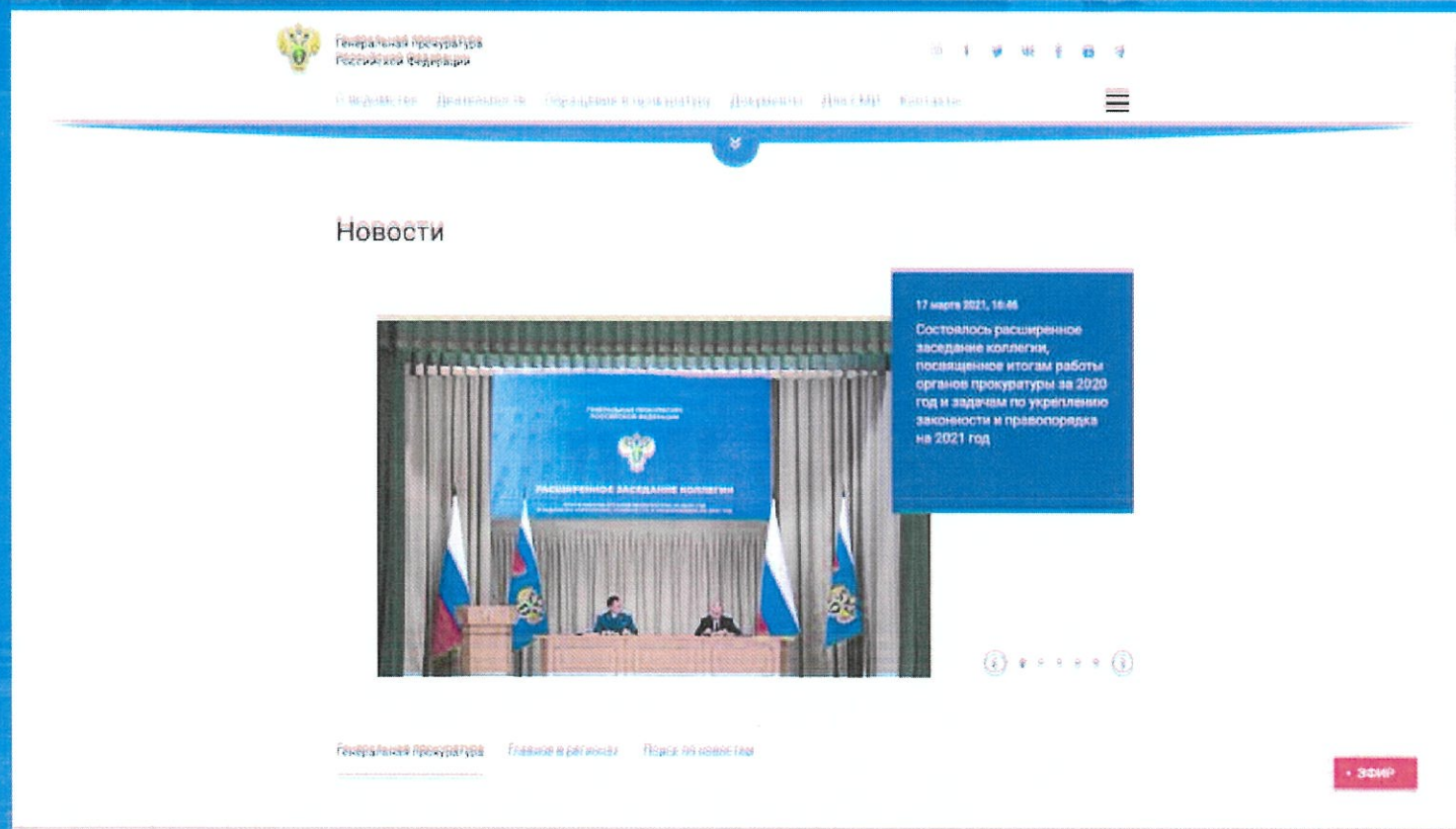
Пресечено функционирование вредоносных ресурсов в зарубежном адресном пространстве

68 420



DDoS-атаки в период проведения несанкционированных акций протеста

Объекты компьютерных атак 23 января 2021 г.



МИД



Минэкономразвития



Минтруд



Росгвардия



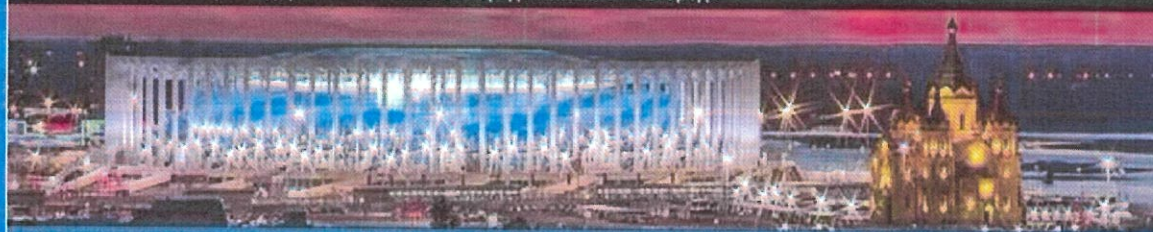
Генпрокуратура



Компьютерная атака на ЦОДД Нижнего Новгорода



Центр Организации Дорожного Движения города Нижнего Новгорода.
Департамент транспорта и дорожного хозяйства города Нижнего Новгорода

[Главная](#)[Направления работы](#)[МКУ «ЦОДД»](#)[Нормативные документы](#)[Обратная связь](#)

Телефонная линия по вопросам организации дорожного движения

Телефон линии по вопросам организации дорожного движения (применение дорожных знаков, светофоров, разметки, ограждений и искусственных неровностей) *

8 920 291 98 49

* Время работы: Понедельник - Четверг 8.00-17.00 Пятница 8.00-16.00

Информация о работе светофорных объектов на 24 марта 2021 года

▲ ул. Лескова – ул. Янки Купалы	Отключение электропитания с 09.00 до 11.00
▲ ул. Б.Печерская около дома №19	Отключение электропитания с 09.00 до 17.00
▲ ул. Алексеевская – переулок Холодный	Отключение электропитания с 09.00 до 17.00
▲ ул. Звездинка в районе дома №32	Отключение электропитания с 09.00 до 17.00



Защита национального информационного пространства в новых реалиях 2020-2021 гг.

Москва. 27 апреля 2021 г.