

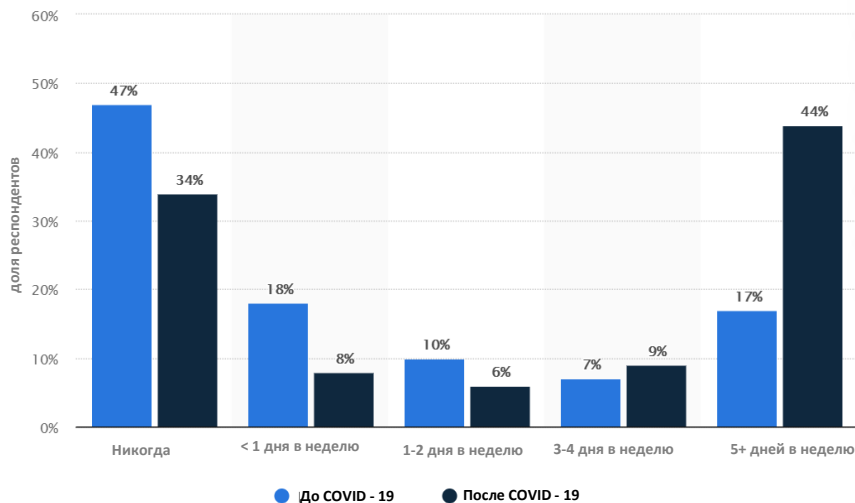
COVID 19: как обеспечить
непрерывность
деятельности в
виртуальном мире



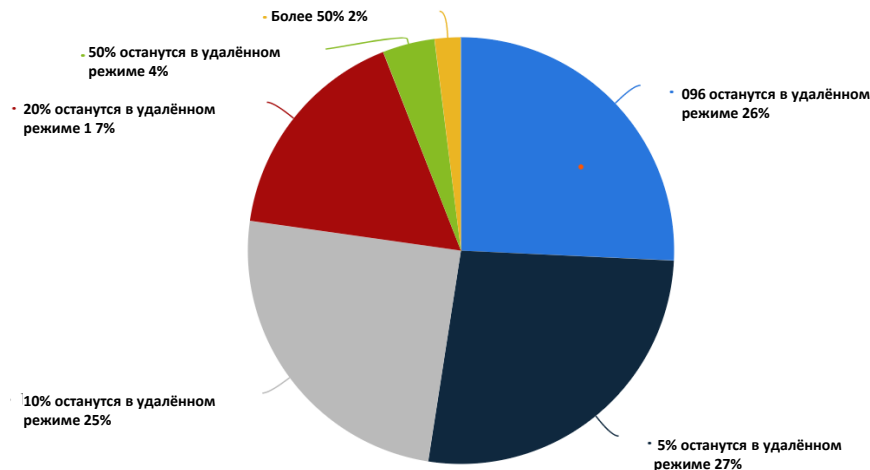
CONTENT



Динамика тенденций в сфере удалённой работы, обусловленной COVID-19, в 2020 г.



Какая часть ваших сотрудников из числа тех, кто не работал удалённо до COVID, продолжит постоянно работать в удалённом режиме после окончания эпидемии?



СТАТИСТИКА: 7 УДИВИТЕЛЬНЫХ ФАКТОВ О ПЕРЕХОДЕ НА УДАЛЁННУЮ РАБОТУ

- 1. Отмечается масштабная «миграция» в пользу работы из дома.** 88% организаций рекомендовали своим сотрудникам или обязали их работать из дома; 91% коллективов в странах Азиатско-Тихоокеанского региона ввели режим работы из дома после начала пандемии. [\[i\]](#)
- 2. Коронавирус стал катализатором удалённой работы.** 31% респондентов заявили, что именно из-за коронавируса (COVID-19) в их компании стали позволять работать удалённо. [\[iii\]](#)
- 3. Организации мобилизуются, используя группы управления в кризисной ситуации для координации своих мер реагирования.** 81% компаний сейчас имеют группы кризисного реагирования. [\[iiii\]](#)
- 4. Больше всего высшее руководство беспокоит обеспечение непрерывности бизнеса.** 71% руководителей обеспокоены непрерывностью бизнеса и производительностью в период пандемии. [\[iv\]](#)
- 5. Киберпреступники пользуются кризисом.** В течение суток Microsoft выявил [масштабную кампанию фишинга](#), в которой использовались 2300 разных интернет-страниц в виде приложений к сообщениям; они были замаскированы под информацию о финансовой компенсации в связи с COVID-19; переходя по ссылке, пользователь попадал на поддельную страницу регистрации Office 365. [\[viii\]](#)
- 6. Недостатки технологии и инфраструктуры – одни из основных препятствий для подключения к сети и производительности труда.** 54% руководителей отделов кадров отметили, что главным препятствием для эффективной удалённой работы в их организации является низкий уровень технологии/инфраструктуры. [\[ix\]](#)
- 7. Удалённая работа – это надолго!** 74% компаний планируют более активно использовать этот режим работы на постоянной основе после окончания пандемии. [\[xv\]](#)

Примеры

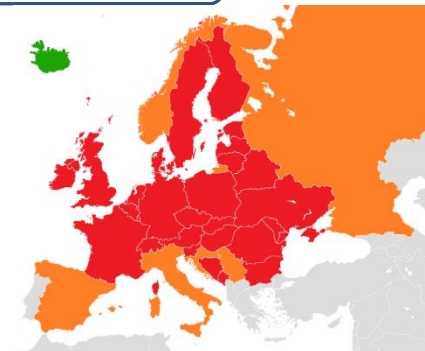
11 сентября 2001 США



11 марта 2011, Япония, ущерб - \$309 млрд



Вулкан Эйяфлатлайокудль
14 апреля 2010, Северная Европа



Ураган «Катрина»
август 2005, США, ущерб - \$125 млрд





43% американских компаний **не возобновляют деятельность** после возникновения чрезвычайной ситуации, ещё 29% прекращают её в течение 3 лет.



20% малых и средних компаний становятся жертвами **крупной чрезвычайной ситуации** каждые 5 лет.



78% организаций, которые не имели планов действий в нештатных ситуациях, понесли катастрофические потери и прекратили деятельность в течение 2 лет,... **в большинстве своём были застрахованы, причём многие – на случай перерыва в деятельности!**

(Источники: U.S. National Fire Protection Agency, U.S. Bureau of Labor, Richmond House Group and B2BContinuity.com)

Это нас не касается!



Пример 2018 года: Центральный банк Армении

Центральный банк Армении



ISO 22301 – Системы управления непрерывности бизнеса

Программа аудита/обеспечения уверенности в непрерывности бизнеса -
ISACA

GTAG 10 Управление непрерывности бизнеса - IIA

Инструменты и материалы из «Интернета»

ISO 22301

система менеджмента (управления) непрерывности бизнеса СМНБ

Часть общей системы менеджмента, которая направлена на установление, внедрение, осуществление, управление, мониторинг, анализ, поддержку и постоянное улучшение непрерывности бизнеса

план (обеспечения) непрерывности бизнеса

Набор документированных процедур, которыми организация руководствуется при реагировании, восстановлении, возобновлении деятельности на установленном уровне в случае нарушения деятельности

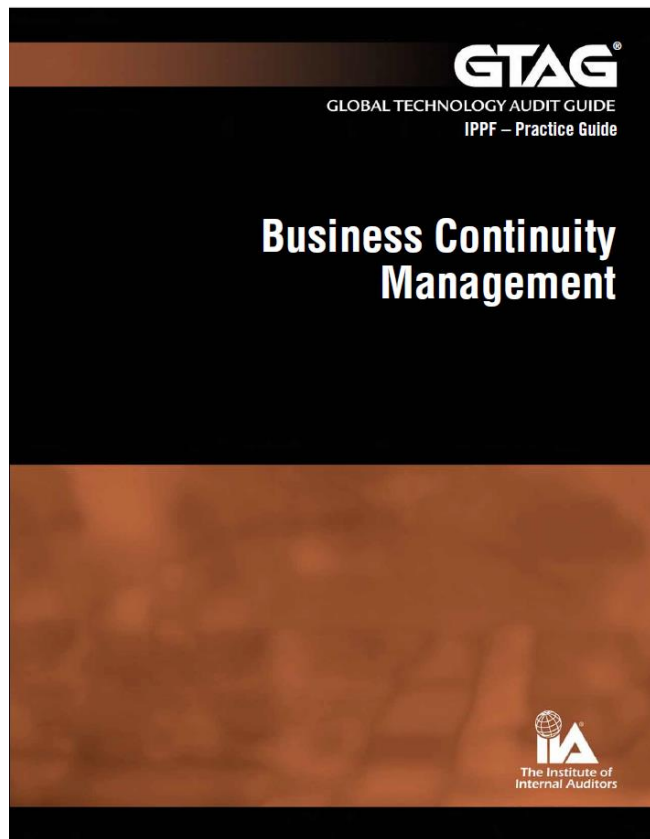
ПРИМЕЧАНИЕ: Обычно охватывает ресурсы, услуги и деятельность, необходимые для обеспечения непрерывности критически важных бизнес-процессов.

анализ воздействия на бизнес

Процесс анализа деятельности и возможного влияния на неё сбоя в функционировании

инцидент

ситуация, которая может произойти и привести к нарушению деятельности, разрушениям, потерям, чрезвычайной ситуации или кризису



Что такое непрерывность бизнеса ?

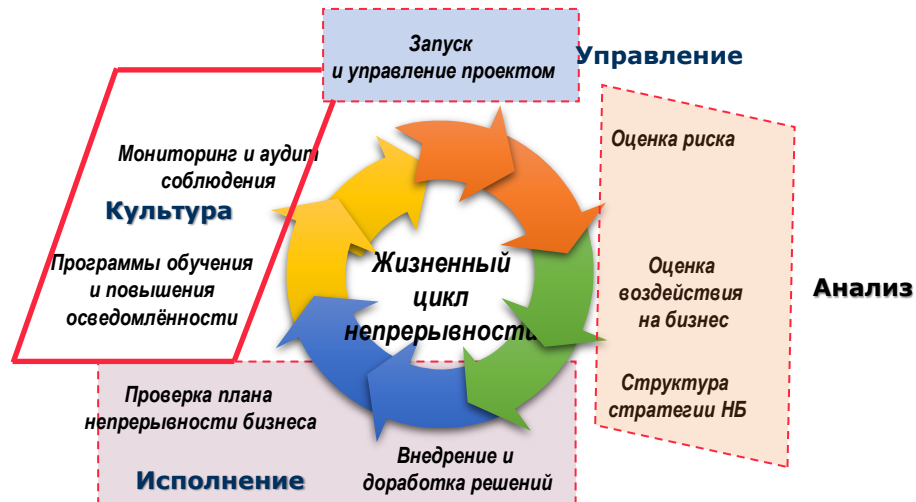
Это способность организации продолжать функционирование с минимальными сбоями или простоями в случае чрезвычайных происшествий, вызванных природными или антропогенными причинами.

Планирование непрерывности бизнеса – стратегическая дисциплина, которая должна быть неотъемлемой частью культуры организации.

??? ПНБ или УНБ ???

Непрерывный процесс, который поддерживается высшим руководством и финансируется, чтобы обеспечить принятие всех необходимых мер для выявления последствий потенциального ущерба, поддержания реалистичных стратегий и планов восстановления, а также обеспечить непрерывность функционирования посредством обучения персонала, проверки плана и технического обслуживания.

Жизненный цикл УНБ



Когда случается нештатная ситуация, важнее всего сделать следующее:

1. Свести к минимуму потерю данных, сохранив важные данные
2. Обеспечить, чтобы все были в безопасности
3. Восстановить резервные ленточные накопители
4. Оповестить руководителя

Объём допустимых потерь данных при отказе компьютера - это:

1. Целевое время восстановления
2. Целевая точка восстановления
3. Уровень предоставления сервиса
4. Максимально приемлемый простой



ISO 22301:2012, Общественная безопасность – Системы менеджмента непрерывности бизнеса

Целевое время восстановления (RTO)

период времени после инцидента, в течение которого:

- должны быть возобновлены поставки продукции или услуг
- должна возобновиться деятельность
- должны быть восполнены ресурсы

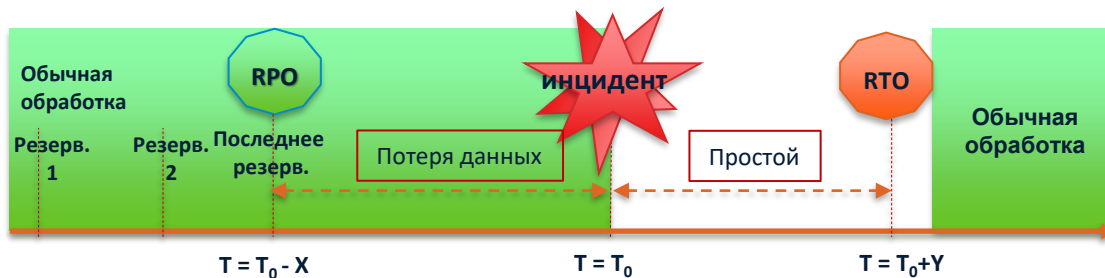
Разрыв в обработке: время, прошедшее с момента сбоя до возобновления обычной обработки.

Целевая точка восстановления

точка на шкале времени относительно сбоя, до которой требуется сохранить данные, используемые в определённой деятельности, чтобы обеспечить выполнение этой деятельности (“максимальная потеря данных”)

Определения ИВА

Данные, которые будут потеряны, уничтожены или иным образом недоступны после успешного восстановления



Ключевые процессы

Процесс	RTO	RPO (периодичность создания резервных копий)
1. Бухучёт и финансы	3 часа	1 час
2. Лицензирование	5 часов	5 дней
3. Государственные платежи	1,5 часа	4 часа
4. Кадры	2 дня	2 недели
5. Связи с общественностью	0,5 часа	2 часа

Пример

Процесс	RTO	RPO (периодичность создания резервных копий)
1. Краткосрочное программирование кредитно-денежной политики. Операции ЦБ на отечественном рынке	3 часа	1 день
2. Операции на международных рынках. Управление валютными резервами	5 часов	0,5 часа
3. Расчёт и публикация обменного курса	1,5 часа	1 день
4. Расчёт и публикация банковской процентной ставки	2 дня	2 недели
5. Денежное обращение	0,5 часа	0,5 часа

ГА должен быть способен ответить на следующие простые и важные вопросы, касающиеся непрерывности бизнеса:

Руководство организации понимает нынешний уровень риска для непрерывности деятельности и возможные последствия с учётом масштаба потерь?

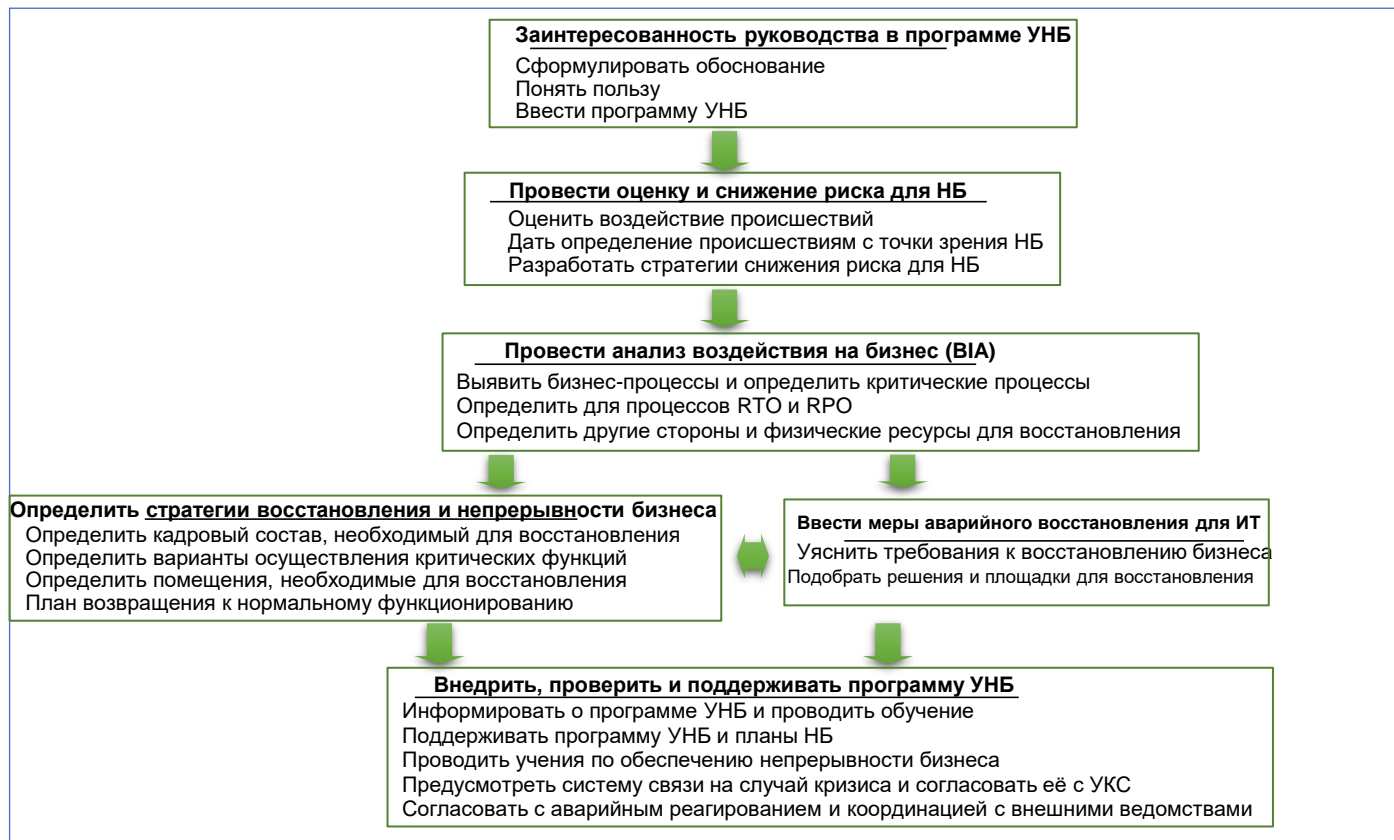
Организация способна доказать, что риски для непрерывности деятельности снижаются до согласованного приемлемого уровня?

Если неприемлемый риск для непрерывности деятельности присутствует, но руководство решает принять его, знают ли владельцы организации и её бизнес-партнёры о том, что руководство решило не снижать этот риск?

Решение принять риск отражено в документах должным образом?



ДЕЙСТВИЯ, НЕОБХОДИМЫЕ ДЛЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ УНБ



КОНТРОЛЬНЫЙ СПИСОК АУДИТА УНБ

1. Управление
2. Анализ воздействия на бизнес и оценка риска
3. Порядок действий на случай нештатной ситуации
4. Документально зафиксированные планы
5. Обучение и тестирование
6. Пересмотр и актуализация



BCM Audit checklist.docx



FBI: Covid-19 Cyberattacks Spike 400% in Pandemic

Online crimes reported to the FBI roughly quadrupled since the coronavirus (Covid-19) pandemic, senior cybersecurity official said.

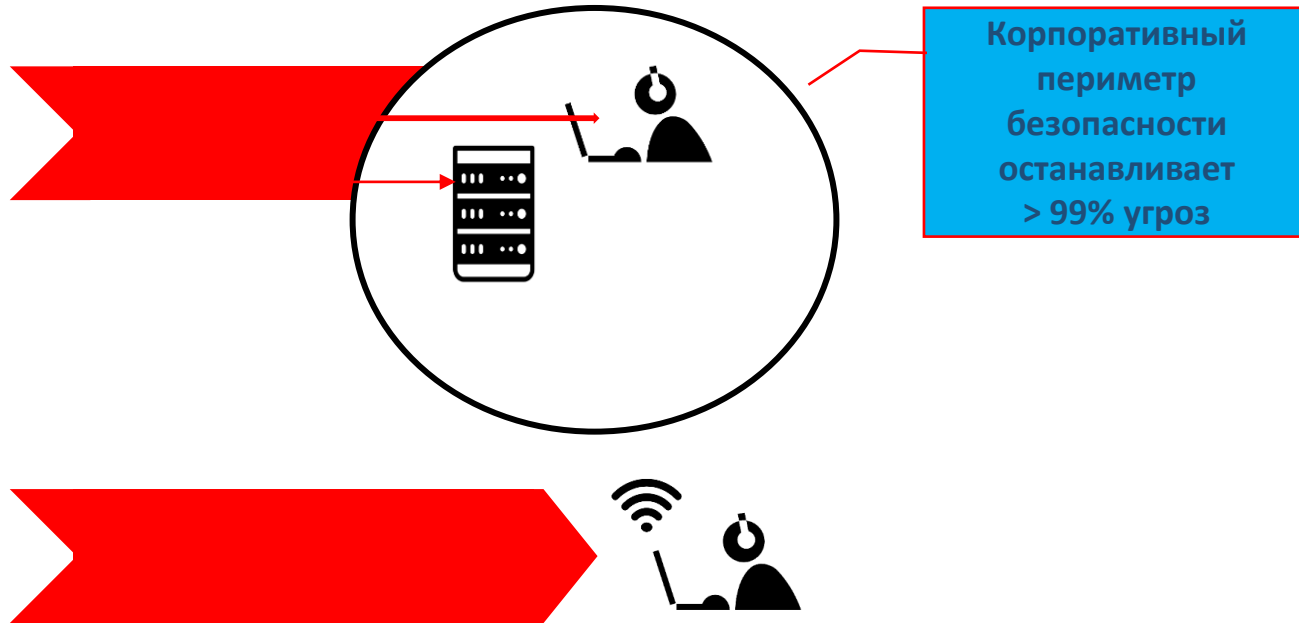


by DH Kass • Apr 19, 2020

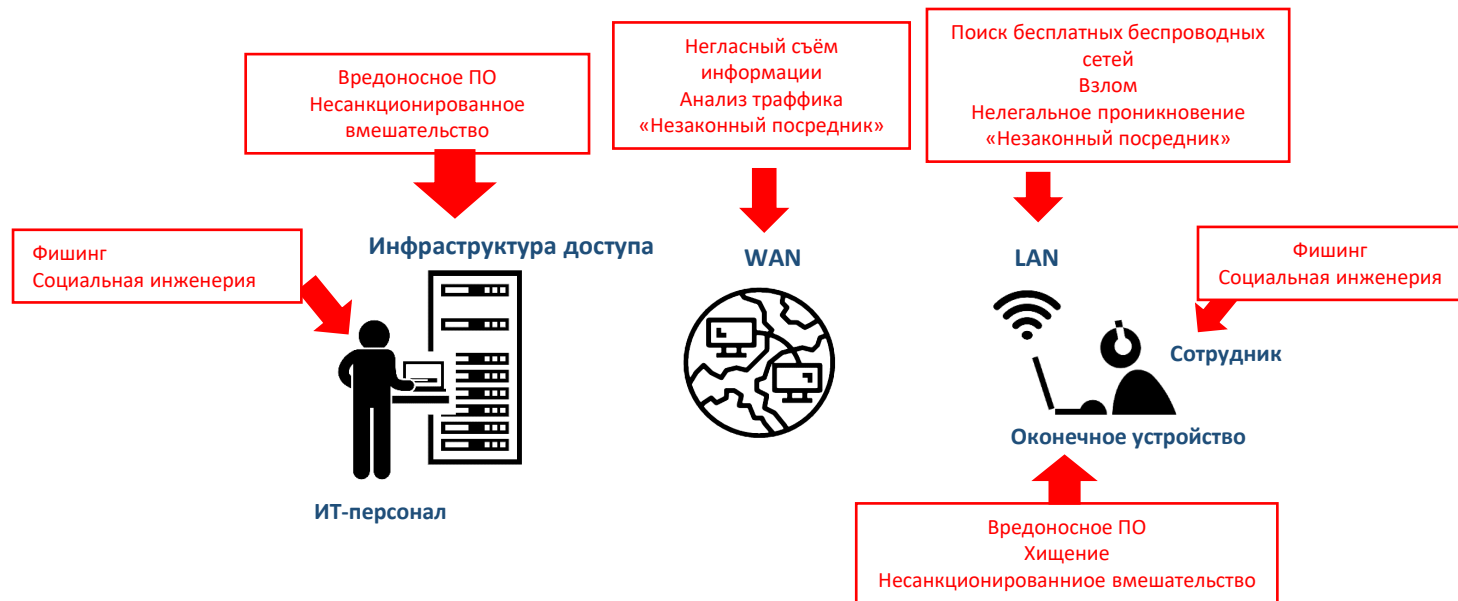
Online crimes reported to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) have roughly quadrupled since the coronavirus (Covid-19) pandemic, a senior cybersecurity official said in a webinar hosted by the Aspen Institute last week.

The number of cybersecurity complaints to the IC3 in the last four months has spiked from 1,000 daily before the pandemic to as many as 4,000 incidents in a day, said Tonya Ugoretz, the deputy assistant director of the FBI's cyber wing, [The Hill](#) reported.

ЗА ПРЕДЕЛАМИ ПЕРИМЕТРА ОПАСНО!



УГРОЗЫ ПРИ УДАЛЁННОЙ РАБОТЕ



Риск: ФИШИНГ

- **91%** успешных попыток организовать утечку данных начинались с фишинговой атаки
- **23%** из тех, кто стал объектом воздействия, открывали фишинговые сообщения, пришедшие по электронной почте, а **11%** нажимали на ссылки или открывали файлы, присланные в приложениях



РИСК: СЛАБАЯ ИНФРАСТРУКТУРА

- Не предназначена для интенсивного и длительного использования
- Недостаточные возможности
 - Малое число одновременных пользователей
 - Малое количество ноутбуков и мобильных устройств
 - Ограниченная пропускная способность
 - Недостаточная поддержка
- От ИТ-департаментов требуют быстро найти решения



РИСК: ОБЛАЧНЫЕ ТЕХНОЛОГИИ

- **Бизнес:** Нам не хватает возможностей для проведения совещаний. Сделайте что-нибудь. И побыстрее!
- **ИТ:** Не, больше серверов быстро ввести не получится... А может, через облако?
- **Бизнес:** Да нам уже вчера нужно было!
- **ИТ:** Ну...ладно, давайте тогда через Zoom!



НЕУДОВЛЕТВОРИТЕЛЬНАЯ СТРУКТУРА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Некоторые критически важные данные передавались через Китай, даже когда в этом не было необходимости



New programme against COVID-19

UN

<GOV UK Notify>

GOV.UK

The government has taken new measures to prevent the spread of disease in law

As a precaution measure against the spread of COVID-19, the Department of Health and Social Care has announced a new refund programme for dental services.

You are eligible to get a tax refund for dental services.

[Access your funds now](#)

The funds can be used to pay for dental services. For more information, visit <https://www.nhs.uk/conditions/coronavirus/> (against corona)

At 6.15pm on 5 March 2020, the Department of Health and Social Care adds COVID-19 to the list of notifiable causative agents.

Coronavirus (2019-nCoV) Safety Measures

DL

@who-pc.com>

COVID-19 urgent help

From: 1234@johnsmith.mn

01/03/2020

COVID-19

Dear Joan,

This is an instruction from the Director-General of the WHO. Please open the attachment for the purpose of receiving updated instructions on how to fight the coronavirus - what common drugs to take for a fast cure to coronavirus. It can be done! You can save your family members and friends so pass it on. And we can help them fight this deadly virus.

DOWNLOAD



ing the spreading of corona virus.

partners to rapidly expand scientific knowledge on this new prevent the spread of this outbreak.

ough, shortness of breath, and breathing difficulties.

- Органам власти и компаниям следует в приоритетном порядке обратить внимание на:
 - Чёткую политику в области удалённого доступа (кто, что, когда и каким образом)
 - Надёжную аутентификацию пользователей и устройств
 - Эффективные методы шифрования
 - Безопасные устройства, с которых осуществляется удалённый доступ (безопасность оконечных устройств)
 - Контроль сетевой безопасности
- В основе использования облачных технологий должна лежать детальная оценка риска
- Следует проводить дополнительные кампании информирования пользователей
- Надёжные средства контроля в отношении конфигурации на обеих сторонах соединения
- Дополнительные меры контроля безопасности в отношении критически важных функций

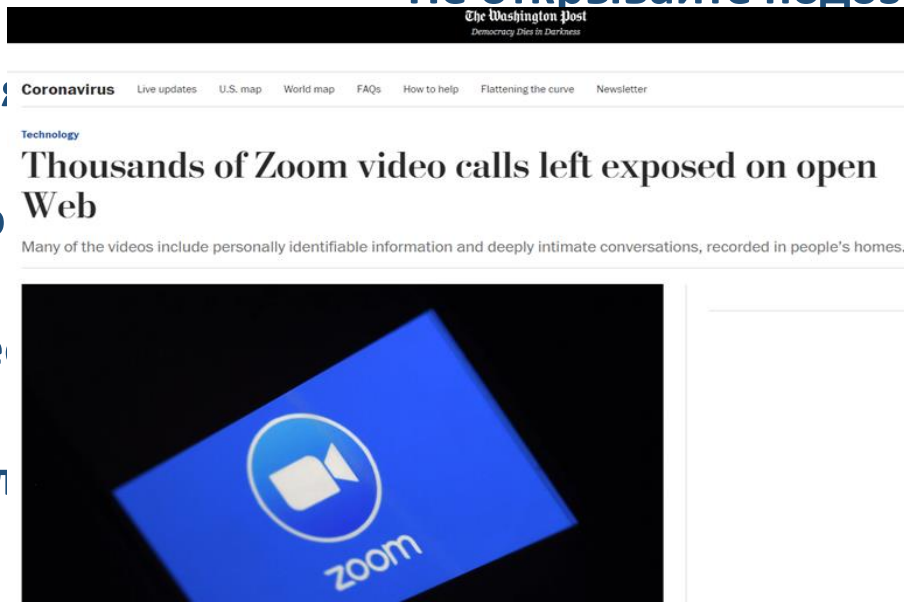
Не открывайте подозрительный контент

Выбирайте подход

Защищайте беспро

Разделяйте рабоче

Регулярно устанавли



ру, когда не

щищайте

ясное место

адёжные пароли /
ую аутентификацию

Защищайте видеоконференции

И ПОСЛЕДНЕЕ...

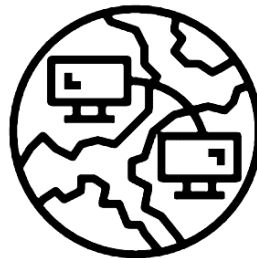
Инфраструктура доступа

WAN

LAN

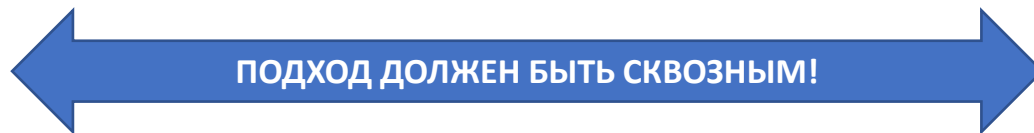


ИТ-персонал



Сотрудник

Оконечное устройство



Thank You