ПРОСТРАНСТВО РЕШЕНИЙ ДЛЯ РАЗВИТИЯ ИННОВАЦИЙ

ПРОСТРАНСТВО РЕШЕНИЙ ДЛЯ РАЗВИТИЯ ИННОВАЦИОННОГО ПОТЕНЦИАЛА СОНКО В СОЦИАЛЬНОЙ СФЕРЕ

ЦЕНТР ГРАНИ

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ

Информационная безопасность на «удаленке»

Тимофей Дубровских
Ольга Шилова
Центр ГРАНИ

Ведущий — Тимофей Дубровских

Системный администратор Центра ГРАНИ

Активист

Амбассадор информационной безопасности

Почему мы об этом говорим?

Переходя на удаленку, компании открывают хакерам доступ к своим серверам

- Из-за спешного массового перехода компаний на удаленную работу стремительно растет число корпоративных серверов, доступных для злоумышленников из интернета – сообщили 27 марта 2020 года эксперты центра мониторинга и реагирования на киберугрозы Solar JSOC. Одна из главных причин – применение компаниями незащищенных протоколов.
- По данным Solar JSOC, всего за одну неделю количество устройств, доступных из интернета по незащищенному протоколу RDP, выросло на 15% в России (общее число на сегодня более 76 тыс. единиц) и на 20% в мире (более 3 млн единиц).

Злоумышленники могут получить доступ к каждому десятому открытому удаленному рабочему столу

- 27 марта 2020 года компания Positive Technologies сообщила о том, что в ходе мониторинга актуальных угроз (threat intelligence) эксперты компании выяснили, что число сетевых узлов в России, доступных по протоколу удаленного рабочего стола (RDP) всего за три недели (с конца февраля 2020 года) увеличилось на 9% и составило более 112 000. Уже сейчас свыше 10% таких ресурсов уязвимы для ошибки безопасности BlueKeep (CVE-2019-0708), которая позволяет взломщику получить полный контроль над компьютером на базе Windows.

Как предотвратить?

Правила

Шаг 1. Сформируйте перечень конфиденциальных документов и данных

- Определите, какие сведения нужно контролировать, чтобы обеспечить информационную безопасность.
- Когда утвердите окончательный перечень, закрепите его внутренним нормативным документом — «Перечень информации, имеющей ограниченный доступ».
- В дополнение к перечню информации, создайте правила, регулирующие информационную безопасность. Например, «Правила работы с финансовой документацией и сведениями, носящими конфиденциальный характер».

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Шаг 2. Установите круг лиц, которые имеют допуск к финансовым сведениям

- Проанализируйте, кому из сотрудников компании для работы нужен доступ к конфиденциальным данным.
- Выделите тех, кому требуется постоянный допуск, а для остальных работников пропишите правила доступа к данной информации.

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Шаг 3. Проведите инструктаж удаленных работников в сфере информационной безопасности

- Чтобы поддерживать дисциплину, можно даже установить штрафы и взыскания за нарушение правил.

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Шаг 4. Используйте технические решения, которые позволят специалистам по безопасности контролировать сотрудников

- Совет весьма спорный, но допустимый , когда удаленный сотрудник работает на корпоративном ноутбуке.
- Либо просто не давать в руки того, кто работает удалённо, ценных конфиденциальных документов.
- Самые быстрые и простые меры,которые вы можете предпринять: Установите пароли для документов и папок сократите набор прав

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Шаг 5. Контролируйте смену паролей и ключей

- Чтобы усилить меры безопасности, периодически меняйте электронные ключи и пароли от учетной системы, электронной почты сотрудников.
- Если увольняете работника или меняете его обязанности, смените все пароли, к которым он имел доступ, и проконтролируйте, чтобы он сдал все электронные носители.

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Как предотвратить?

Программы

- Установить систему проверки всех процессов, выполняемых подключенным компьютером. Таким образом, можно будет остановить кибер-атаки, которые не используют вредоносные программы , а также сложные и неизвестные атаки, благодаря которым злоумышленники могут проникнуть в корпоративную сеть через компьютер сотрудника без его ведома.

- Соединение между компьютером и корпоративной сетью всегда должно быть защищено с помощью VPN (виртуальной частной сети). Такая частная сеть позволяет создавать защищенную локальную сеть без необходимости физического подключения ее участников друг к другу.

- Пароли, используемые для доступа к корпоративным службам, и пароли сотрудников в целом должны быть сложными и трудными для расшифровки.

- Важно использовать многофакторную аутентификацию (MFA). Благодаря этой двойной системе проверки доступа, можно более эффективно защитить доступ к VPN, к логинам сотрудников для корпоративных порталов и ресурсов, к облачным приложениям. Она даже поможет соблюдать требования по защите данных.

- Системы межсетевого экрана, будь то виртуальные или физические, являются первой линией защиты в корпоративной сетевой безопасности. Эти системы отслеживают входящий и исходящий трафик и принимают решение о блокировке или разрешении определенного трафика на основе набора ранее определенных политик безопасности.

- Службы мониторинга для сетей, приложений и пользователей, а также службы реагирования и устранения возможных сбоев также необходимы для мониторинга и обеспечения непрерывности работы при удаленной работе его сотрудников.

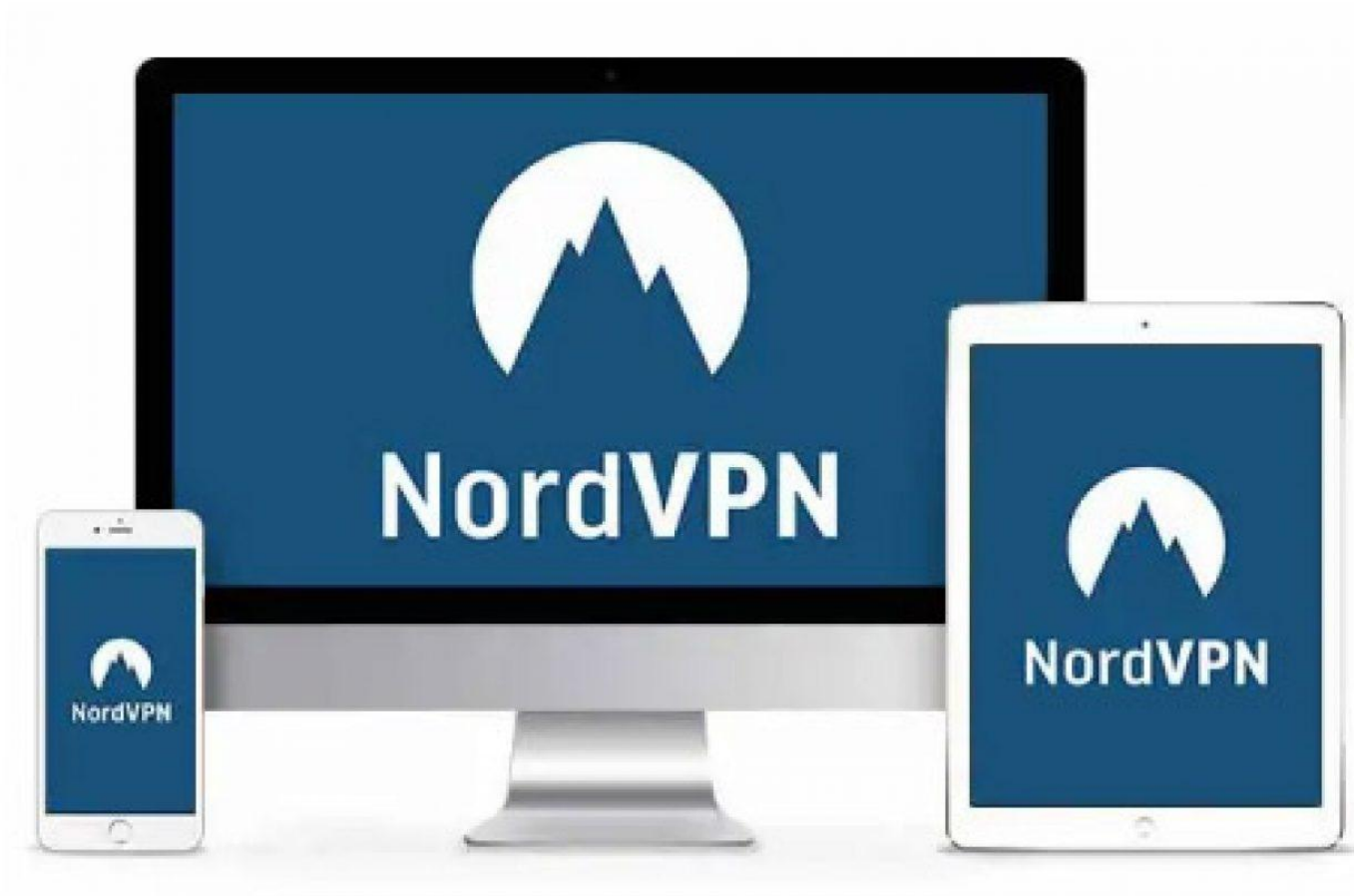
Что мы сделали у себя?

- Двойная аутентификация
- VPN на все устройства (или почти на все)
- Шифрование
- Использование безопасных мессенджеров
- Запрет на передачу документов через социальные сети
- Хитрости в ZOOM, для отсечения троллей

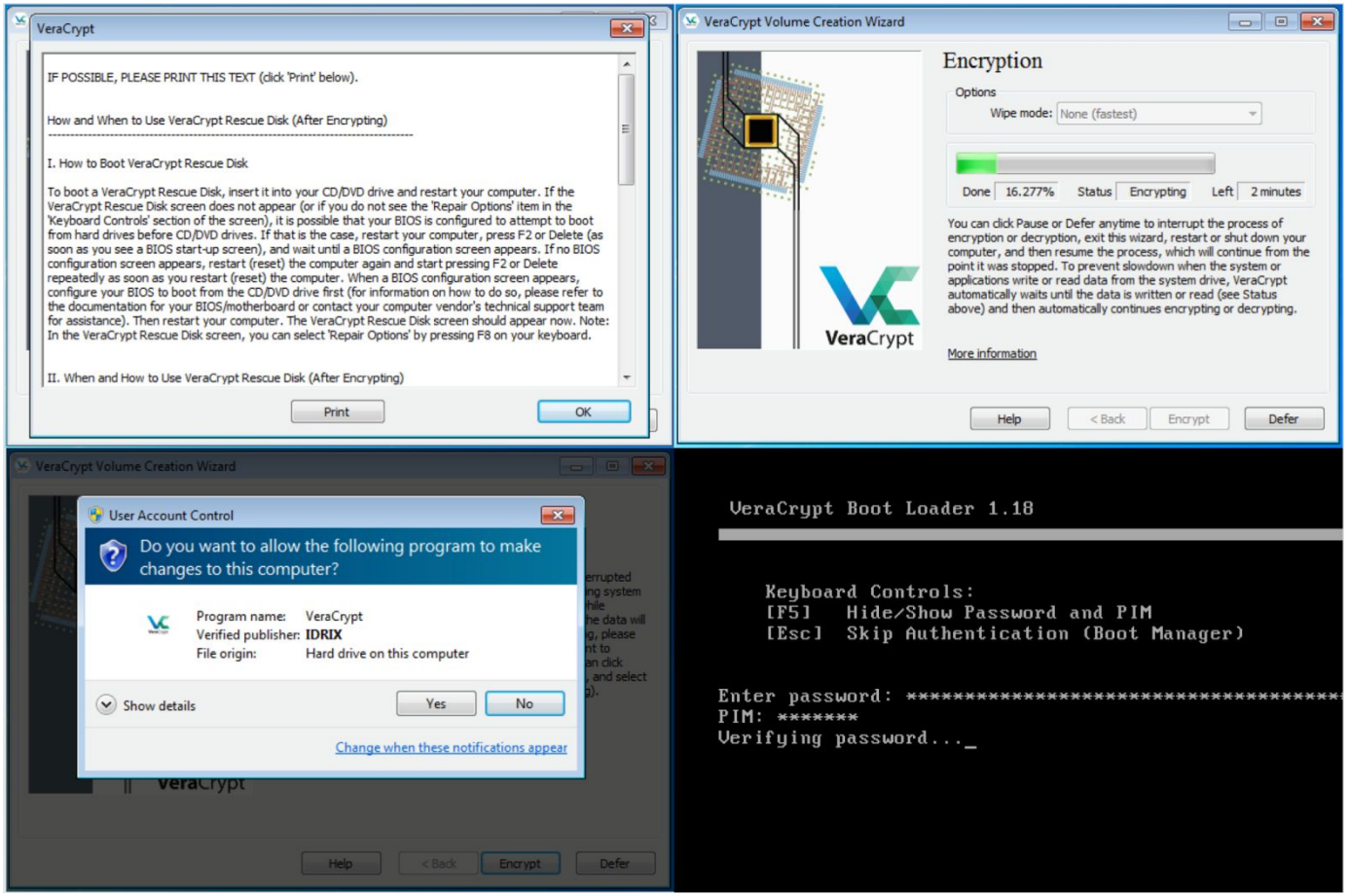
Пандемия запустила процесс глобальной вынужденной цифровизации. Сколково

Что защищаем

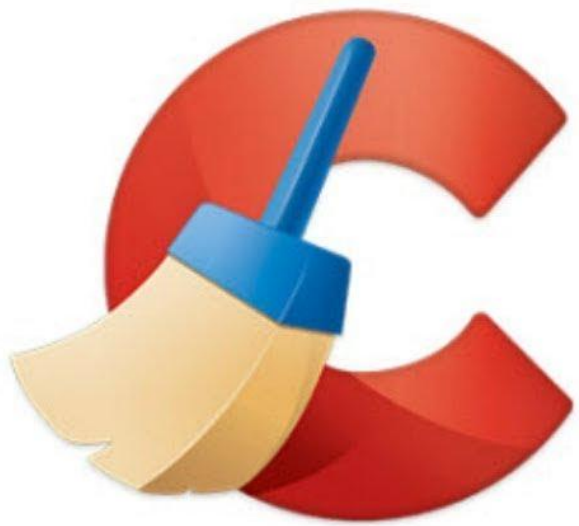
- Веб-Сервер — Данные сервера
- Электронные почты — Данные переписок (особенность пользовательских соглашений yandex.ru, mail.ru)
- Сайт, старый сайт — Данные на сайте (что может случиться с заброшенным сайтом, почему важна антивирусная защита сайтов)
- Группы в социальных сетях — Данные социальных сетей
- Конференции в ZOOM — данные конференций


NordVPN
NordVPN
NordVPN

Шифрование


VeraCrypt
IF POSSIBLE, PLEASE PRINT THIS TEXT (click 'Print' below).
How and When to Use VeraCrypt Rescue Disk (After Encrypting)
I. How to Boot VeraCrypt Rescue Disk
To boot a VeraCrypt Rescue Disk, insert it into your CD/DVD drive and restart your computer. If the VeraCrypt Rescue Disk screen does not appear (or if you do not see the 'Repair Options' item in the 'Keyboard Controls' section of the screen), it is possible that your BIOS is configured to attempt to boot from hard drives before CD/DVD drives. If that is the case, restart your computer, press F2 or Delete (as soon as you see a BIOS start-up screen), and wait until a BIOS configuration screen appears. If no BIOS configuration screen appears, restart (reset) the computer again and start pressing F2 or Delete repeatedly as soon as you restart (reset) the computer. When a BIOS configuration screen appears, configure your BIOS to boot from the CD/DVD drive first (for information on how to do so, please refer to the documentation for your BIOS/motherboard or contact your computer vendor's technical support team for assistance). Then restart your computer. The VeraCrypt Rescue Disk screen should appear now. Note: In the VeraCrypt Rescue Disk screen, you can select 'Repair Options' by pressing F8 on your keyboard.
II. When and How to Use VeraCrypt Rescue Disk (After Encrypting)
Print
OK
VeraCrypt Volume Creation Wizard
Encryption
Options
Wipe mode: None (fastest)
Done 16.277% Status Encrypting Left 2 minutes
You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, VeraCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.
VeraCrypt
More information
Help
< Back
Encrypt
Defer
VeraCrypt Volume Creation Wizard
User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: VeraCrypt
Verified publisher: IDRIX
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear
VeraCrypt
Help
< Back
Encrypt
Defer
VeraCrypt Boot Loader 1.18
Keyboard Controls:
[F5] Hide/Show Password and PIM
[Esc] Skip Authentication (Boot Manager)
Enter password:
PIM: ********
Verifying password...


ESET
NOD32
ANTIVIRUS
eset



CCLEANER

Чек лист безопасности

1.	Для удалённой работы используются защищенные каналы связи, например, при помощи VPN (Virtual Private Network)?	
2.	При подключении к инфраструктуре пользователь проходит двухфакторную аутентификацию (токены, одноразовые пароли)?	
3.	При удалённом подключении не используются личные устройства сотрудников?	
4.	На удалённых рабочих местах контролируются съемные носители, запрещен «прямой» доступ в сеть интернет?	
5.	При подключении к сети компании происходит проверка удалённых устройств на наличие антивируса и его актуальности и на наличие необходимых обновлений безопасности?	
6	Использование корпоративных сервисов разрешено только со специально сконфигурированных «джамп-узлов»: терминальных серверов, виртуальных рабочих столов (VDI)?	
7.	В ИТ-инфраструктуре компании выполнено сегментирование и настроены разграничения доступа, пользователи имеют минимальный для работы набор прав?	
8.	В ИТ-инфраструктуре компании определены и применяются политики информационной безопасности и аудита событий?	
9.	Обеспечивается ли постоянный мониторинг и реагирование на события безопасности для обнаружения и предотвращения компьютерных атак и инцидентов, до того момента, как они могут вызвать реальные негативные последствия для компании?	
10.	Выполняется ли контроль изменений состава ресурсов, для которых предоставлен удалённый доступ, анализ защищенности сетевого периметра и инфраструктуры, обнаружение и устранение уязвимостей и ошибок настройки	

Распространенные опасности

Фишинговые компании

- электронные письма на тему коронавируса , чтобы попытаться обманным путем заставить пользователей скачать и запустить вредоносные программы.
- рассылка от лица государственных учреждений, отправляющих информацию о вирусе;
- рассылка информации о возможностях заказов на покупку масок для лица в целом СИЗ
- Сайты с необходимостью ввода адреса электронной почты и другой личной информации

Не вводите свои данные на незнакомых сайтах

Общеизвестная информация.

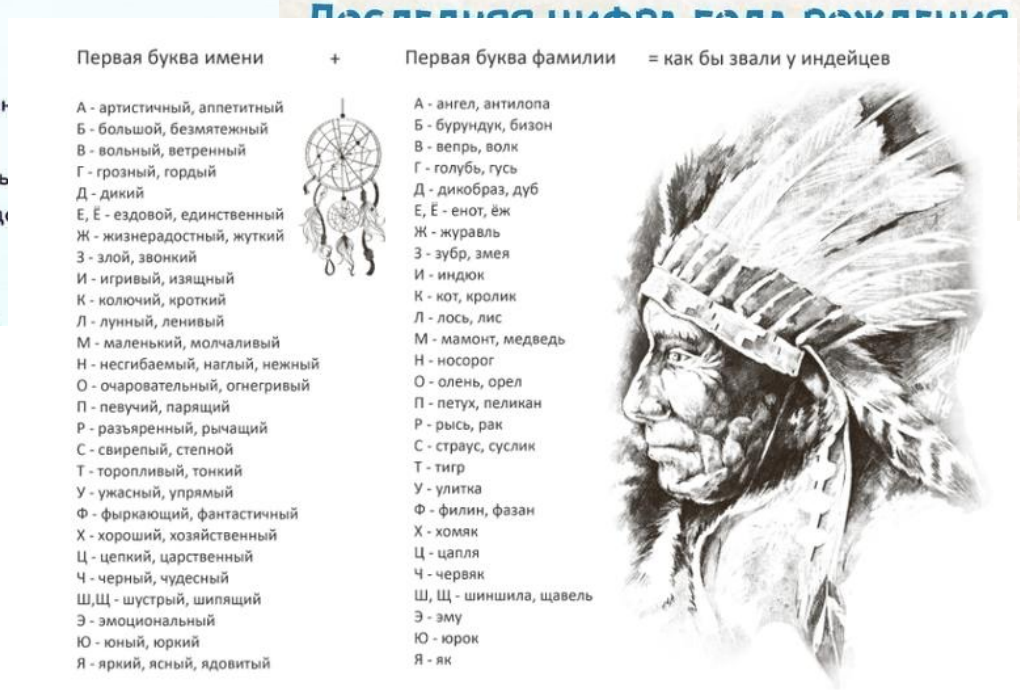
Дополним

- Старайтесь не использовать менеджер паролей на устройствах,
- где нет антивирусной защиты
- Где больше одного пользователя

- В последнее время появилось много «игр», когда надо

- подобрать свое индейское имя.
- название фильма, который бы характеризовал вашу жизнь
- И т.д.

Иногда, это просто игра, а иногда – **способ собрать информацию для подбора данных о пользователях.**



Безопасность может стоить дешево, на заплатить за нарушение ее правил придется дорого

«Информационная безопасность» — это процесс обеспечения доступности, целостности и конфиденциальности информации.

ПРОСТРАНСТВО РЕШЕНИЙ ДЛЯ РАЗВИТИЯ ИННОВАЦИЙ

ПРОСТРАНСТВО РЕШЕНИЙ ДЛЯ РАЗВИТИЯ ИННОВАЦИОННОГО ПОТЕНЦИАЛА СОНКО В СОЦИАЛЬНОЙ СФЕРЕ

НА ГРАНИ ВОЗМОЖНОГО
ЦЕНТР ГРАНИ

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ

Спасибо за внимание

www.grany-center.org