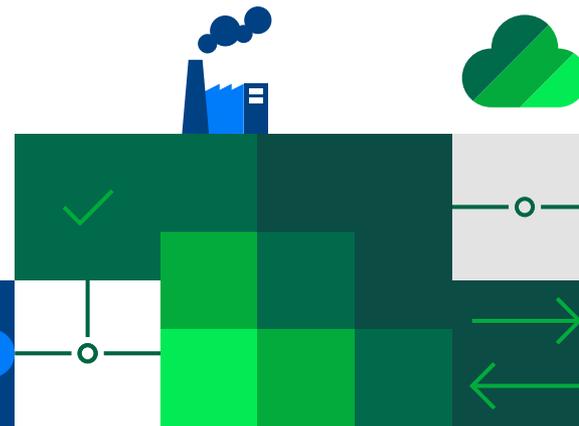




Обеспечение ИБ при удаленной работе предприятия

Андрей Голов

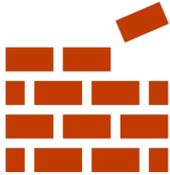


Неготовность инфраструктуры

- Перегрузка систем удаленного доступа
- Отсутствие ноутбуков
- Проблемы с обновлением удаленных АРМ

Неготовность процессов

- Использование небезопасных средств
- Сложность контроля удаленных пользователей
- Отсутствие политики



Невозможность
создания
периметра



За компьютером
работают
посторонние



Повышенная
уязвимость к
фишингу в условиях
пандемии





Дети за рабочим ПК
(хотелось бы только для
удаленных занятий)



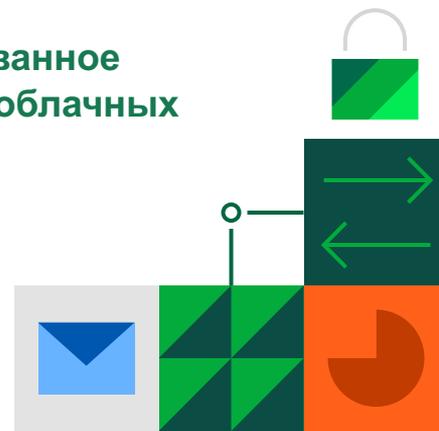
Отсутствие средств
мониторинга активности
удаленных пользователей



Отсутствие средств VPN
и прямое подключение
к RDP-серверу



Несанкционированное
использование облачных
сервисов



Менеджер



Руководитель



ИТ-специалист



Оператор АСУ



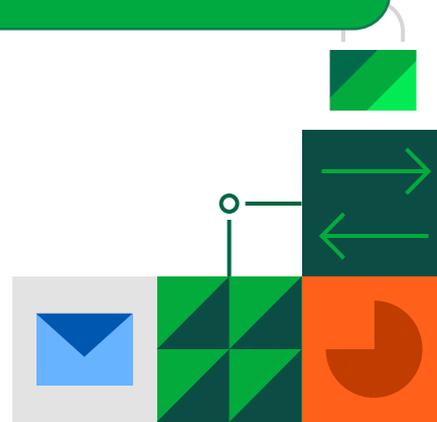
ИСПДн в
коммерческой
организации



Государственная
информационная
система



Значимый объект
КИИ



Усиление атак на удаленных пользователей



Атаки через скомпрометированные облачные сервисы (Zoom, TeamViewer)



Фишинг



Вредоносные веб-сайты

Усиление атак на ИТ-инфраструктуру



Вирусы-шифровальщики



Кража данных



Атаки государственных хакеров



- Ваше решение выдержит 50 удаленных пользователей, а 5000?
- Хватит ли лицензий?
- Как вы проведете нагрузочное тестирование?
- Как вы расширите канал от пользователей до офиса?
- Как вы обеспечите диагностику неполадок?



«Код Безопасности» поможет защитить данные компании во время карантина по коронавирусу

Главная / Новости

16 марта 2020

О компании | VPN | Антивирусная защита | Защита от HCU | Межсетевой экран | Продукт: Континент АП

Эксперты компании «Код Безопасности» (входит в группу компании ЛАНИТ) 19 марта проведут бесплатный семинар «Карантин из-за коронавируса. Что делать безопасности».

Спикеры расскажут, на какие особенности стоит обратить внимание при переводе сотрудников на удаленную работу. Также сотрудниками «Кода Безопасности» разберут ключевые компоненты политики удаленного доступа. Зарегистрироваться на семинар можно по [этой ссылке](#).

В период, когда многие компании переводят сотрудников на удаленную работу, «Код Безопасности» бесплатно даёт лицензии СКЗИ «Континент-АП» и Secret Net Studio пакет «Постоянная защита» сроком на 1 год. Они дают возможность организовать удаленную работу своих сотрудников с максимальным комфортом, без потери контроля над безопасностью данных и ИТ-инфраструктуры.



Компания «Код Безопасности» вносит посильный вклад в борьбу с распространением коронавируса Covid-19

Главная

Пакет «Защищенный удаленный доступ». Быстро, удобно, безопасно!

Публикация: 07 Апрель 2020 - 14:05, редакция: 20.05.2020 12:52



Уважаемые коллеги!

Предлагаем вашему вниманию пакет «Защищенный удаленный доступ», который позволит вам реализовать защищенный удаленный доступ к корпоративным информационным ресурсам в соответствии с требованиями законодательства РФ по ИБ и использовать его в течение первых трех месяцев без оплаты.

18 марта 2020 **НОВОСТИ**

ИнфоТеКС предоставит на безвозмездной основе лицензии на свое ПО для организации защищенного удаленного доступа

В настоящее время компания ИнфоТеКС получает и обрабатывает множество ваших запросов на предоставление лицензий на ПО VIPNet Client с целью организации удаленного защищенного доступа. Выражаем вам глубокую признательность за оказываемое тем самым ваше доверие к нашим продуктам и решениям!

С целью оперативного разрешения всех вопросов и принимая во внимание непростую ситуацию с развитием коронавирусной инфекции мы объявляем о своей готовности предоставить необходимое число лицензий на ПО VIPNet Client, VIPNet Connect, VIPNet IDS HS и VIPNet SafeBoot для расширения защищенных сетей VIPNet всем российским заинтересованным организациям на безвозмездной основе сроком на 6 мес. Указанные лицензии вы можете использовать по своему усмотрению не только для реализации удаленного защищенного доступа, но и для дополнительного сегментирования своих локальных сетей, например, с целью защиты ваших систем IP-телефонии и видеоконференцсвязи для проведения внутренних дистанционных совещаний между своими подразделениями без необходимости очно собирать десятки сотрудников в одном помещении.

23 марта 2020 г.

Решения «Лаборатории Касперского» на полгода стали бесплатными для медицинских учреждений

«Лаборатория Касперского» на полгода* бесплатно предоставит медицинским учреждениям по всему миру лицензии на продукты для защиты от киберугроз.

Речь идёт о корпоративных решениях для конечных устройств и облачных инфраструктур: Kaspersky Endpoint Security Cloud Plus, Kaspersky Security для Microsoft Office 365, Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Security для виртуальных и облачных сред.

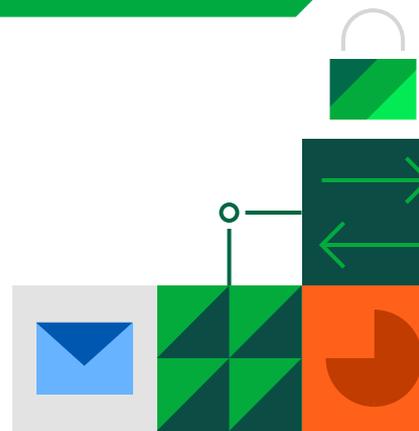


Оперативно обеспечить
подключение

Обеспечить
адекватную
защиту

Адаптировать
бизнес-процессы

Оптимизировать
ИТ-
инфраструктуру



Формирование требований к системе удаленного доступа

- Офисный пользователь
- Топ-менеджер
- Оператор АСУ

- Корпоративный ноутбук
- Собственный компьютер
- Мобильное устройство
- Виртуальный рабочий стол

Пользователь

Устройство

Управление

Приложение

- Обновления ОС
- Средства защиты
- Мониторинг
- Реагирование на инциденты ИБ

- Почта и Интранет-портал
- ERP и другие тяжелые системы
- АСУ ТП
- Онлайн или оффлайн?

Удаленный пользователь

Соответствие
требованиям

Контроль
программной среды

VPN-клиент

Инфраструктура

Сервер удаленного
доступа

Инфраструктура VDI или
терминальный сервер

Проверка трафика
удаленных пользователей

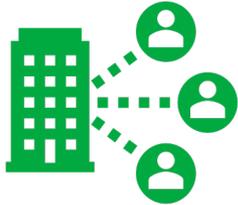
Мониторинг

Мониторинг удаленных
рабочих мест

Реагирование на
инциденты



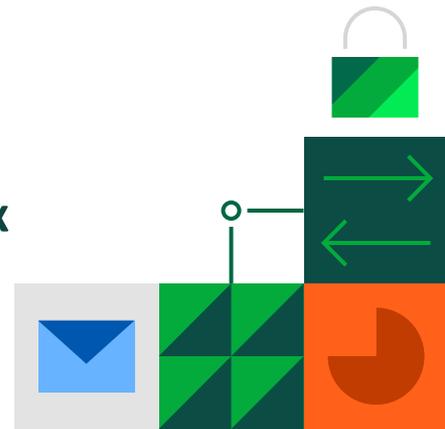
Мониторинг нагрузки на подсистему
удаленного доступа



Мониторинг состояния удаленных
клиентов



Диагностика неполадок удаленных
клиентов







Zero Trust Networking





Гибридный режим работы – прижился



Защитить ИТ-инфраструктуру – возможно



Грамотно сформулированные требования – залог успеха





Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru

