КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

01 ноября 2018 г.
г. Тюмень

#CODEIB

ЗАЩИТА ОТ ВИРУСОВ В СРЕДЕ WINDOWS

ПРОГРАММНЫЕ РЕШЕНИЯ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ

СЕРГЕЙ ЩЕРБАКОВ
АО «СИБНЕФТЕМАШ»

ТЕЛЕФОН: +7 (922) 477-00-27
EMAIL: sherbakov@sibneftemash.ru

ИЗВЕСТНЫЕ ВИРУСЫ

Чернобыль (1999)

также известен как CIH — компьютерный вирус, созданный тайваньским студентом Чэнь Ин Хао в июне 1998 года. Работает только на компьютерах под управлением Windows 95/98/ME. Считается одним из самых опасных и разрушительных вирусов, так как после активации он способен повредить данные микросхем BIOS и уничтожить всю информацию с жёстких дисков. Всего от Чернобыля пострадало около 500 000 персональных компьютеров по всему миру, убытки оцениваются в $ 1 млрд. Автор вируса Чэнь Ин Хао ни разу не привлекался к ответственности и сейчас работает в компании Gigabyte.

I love you (2000)

fff

также известный как **LoveLetter** — компьютерный вирус, который успешно атаковал миллионы компьютеров под управлением Windows в 2000 году.
Вирус был разослан на почтовые ящики с Филиппин в ночь с 4 мая на 5 мая 2000 года; в теме письма содержалась строка «ILoveYou», а к письму был приложен скрипт «LOVE-LETTER-FOR-YOU.TXT.vbs». В большинстве случаев пользователь открывал вложение. При открытии вирус рассылал копию самого себя всем контактам в адресной книге Microsoft Outlook. Он также перезаписывал файлы определённых типов и распространялся через IRC-каналы, создавая файл LOVE-LETTER-FOR-YOU.HTM в системном каталоге Windows. В общей сложности, вирус поразил более 3 миллионов компьютеров по всему миру. Предполагаемый ущерб, который червь нанёс мировой экономике, оценивается в размере 10-15 миллиардов долларов , за что вошёл в Книгу рекордов Гиннесса, как самый разрушительный компьютерный вирус в мире.

- Пользователи, открывавшие файл, тем самым передавали программу дальше, то есть механизм передачи был основан на методах социальной инженерии.
- Расширение файла в системах Windows по умолчанию было скрыто. Таким образом, файл с двойным расширением .txt.vbs пользователями воспринимался как безопасный текстовый файл
- Открытие приложенного к письму файла вызывало немедленное исполнение программы, и вирус получал непосредственный доступ к системе и системному реестру

Melissa (1999)

Эпидемия вируса Melissa началась 26 марта 1999 г. Тогда это был вирус нового типа. Он распространялся по электронной почте в присоединенном файле, и после того как пользователь открывал этот файл, вирус рассылал себя по первым 50 адресам в адресной книги почтовой программы Microsoft Outlook. Он не наносил никакого ущерба самому компьютеру, но порождал лавину новых писем, и из-за перегрузки выходили из строя корпоративные серверы. Ущерб от этого вируса, по некоторым оценкам, достиг миллиарда долларов.
Через неделю после начала эпидемии полиция Нью-Джерси и агенты ФБР вычислили, что вирус был выпущен в Internet с адреса онлайновой службы AOL, принадлежащего некоему 30-летнему Дэвиду Смиту. Он признался в том, что именно он создал вирус Melissa. Он также согласился сотрудничать со следствием, поэтому ему было предъявлено обвинение в нанесении ущерба в размере 80 млн дол. по статье, которая предусматривала тюремное заключение сроком от 46 до 57 месяцев. Потом Смит был выпущен под залог в 100 тысяч дол. и дело начали спускать на тормозах. Слушания неоднократно переносились, и обвинители, так шумно начавшие это дело, теперь хранят молчание. Молчат также сам Джим Смит.

SQL Slammer (2003)

Занимавший всего 376 байт, червь SQL Slammer содержал большое количество разрушений в компактной оболочке. Червь отключал Интернет, колл-центры экстренных служб, 12000 банкоматов Bank of America и отключил от Интернета большую часть Южной Кореи. Червь также смог отключить доступ к глобальной паутине на АЭС в Огайо.

Sobig.F (2003)

Троян Sobig.F инфицировал более 2 миллионов компьютеров в 2003 году, парализовав работу авиакомпании Air Canada и вызвав замедление в компьютерных сетях по всему миру. Данный зловред привел к 37,1 миллиардным затратам на очистку, что является одной из самых дорогих кампаний по восстановлению за все время.

Nimda (2001)

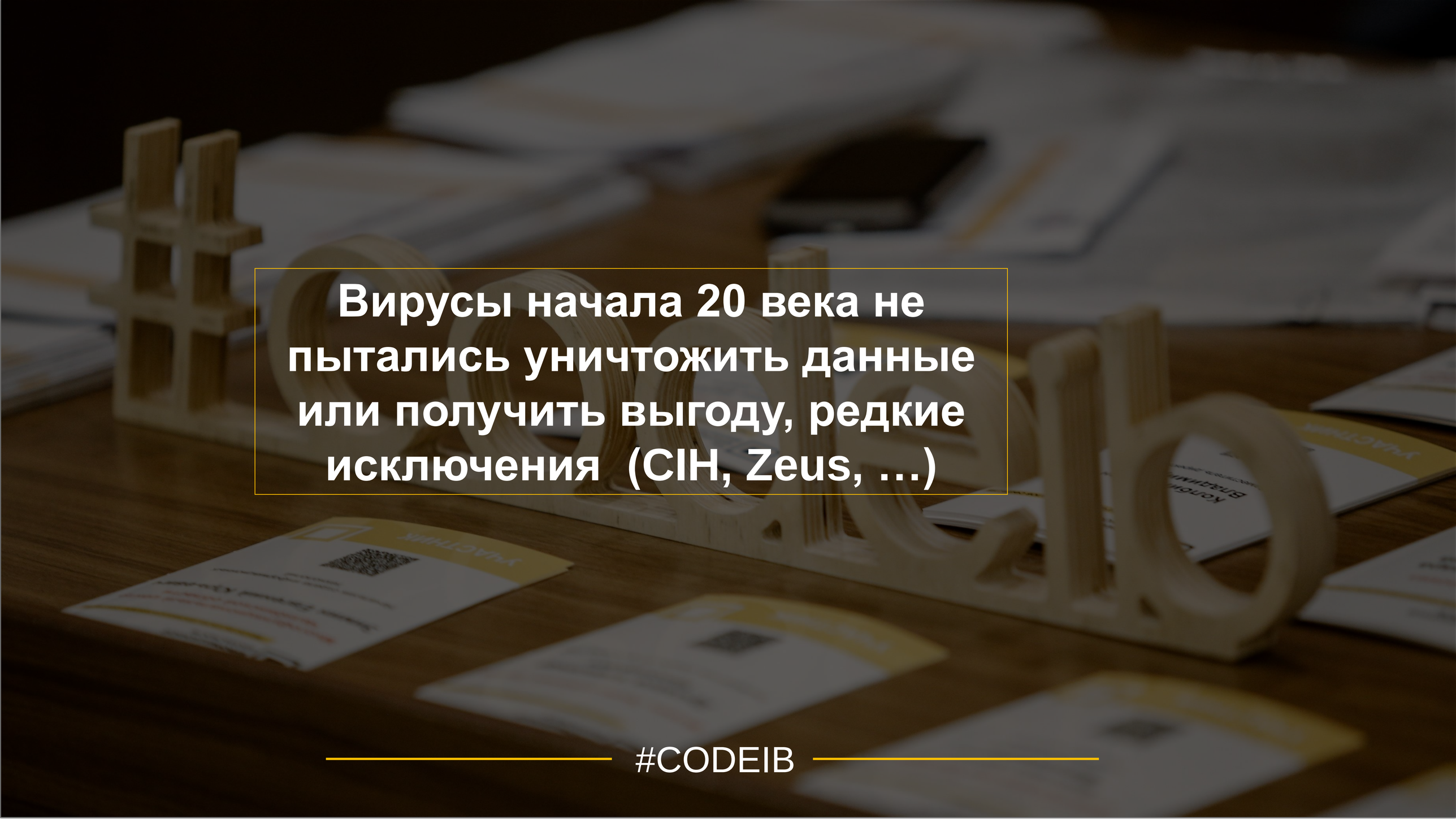
Nimda — компьютерный червь/вирус, повреждающий файлы и негативно влияющий на работу компьютера. Впервые был замечен 18 сентября 2001 года. Название вируса происходит от слова admin, написанного наоборот. Благодаря тому, что червь Nimda использует несколько методов распространения, он в течение 22 минут стал самым распространённым вирусом/червём интернета. Распространяется по электронной почте через уязвимость в Outlook, через открытые сетевые ресурсы, общие папки и передачи файлов, а также через просмотр вредоносных веб-сайтов.

Conflicker (2008)

один из наиболее опасных и известных червей, ориентированный на компьютеры под управлением операционных систем Microsoft Windows. Системы Linux и Macintosh к нему полностью устойчивы. Впервые был обнаружен в сети 21 ноября 2008. К февралю 2009 г. Conficker инфицировал 12 млн. компьютеров по всему миру, в том числе государственных, корпоративных и домашних. 13 февраля 2009, компания Microsoft пообещала награду в 250 000 долларов за информацию о создателях вируса. Была даже создана специальная группа по борьбе с Conficker, которую неофициально окрестили Conficker Cabal. Ущерб, нанесённый вредоносной программой, оценивается в $ 9,1 млрд

Zeus (2009)

В то время как большинство вредоносных программ нашего списка вызывали неприятности Zeus (aka Zbot) изначально был инструментом, используемым организованной преступной группировкой.
Троян использовал приемы фишинга и кейлоггинга для кражи банковских аккаунтов у жертв. Зловред успешно похитил 70 миллионов долларов со счетов жертв.

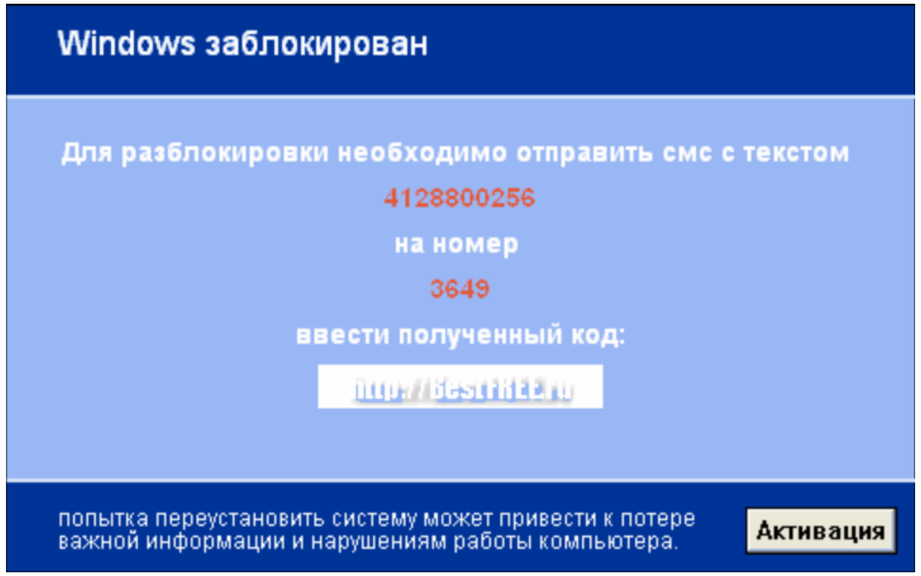


Вирусы начала 20 века не пытались уничтожить данные или получить выгоду, редкие исключения (CIH, Zeus, …)

#CODEIB

ВИРУСЫ ВЫМОГАТЕЛИ (RANSOMWARE)

1 Trojan.WinLock (2007) - блокировка



I тип — это баннеры или порноинформеры, появляющиеся только в окне браузера. Наиболее легко удаляемый тип. Обычно они выдают себя за дополнительные плагины или надстройки для браузера.
II тип — это баннеры, которые остаются на рабочем столе после закрытия браузера и при этом закрывают бóльшую его часть. Но у пользователей обычно остаётся возможность открывать другие программы, в том числе Диспетчер задач и Редактор реестра.
III тип — это тип баннеров, который загружается после полной загрузки рабочего стола Windows. Они закрывают практически весь рабочий стол, блокируют запуск Диспетчера задач, Редактора реестра, а также загрузку в безопасном режиме. Некоторые разновидности полностью блокируют клавиатуру, предоставляя пользователю лишь цифровые клавиши из своего «интерфейса» и рабочую мышь для ввода кода.
IV тип — это тип баннеров, которые прописываются в загрузочный сектор диска (MBR) и блокируют компьютер еще до загрузки Windows. Это так называемый MBR.Lock. Выглядят они все одинаково примитивно, так как выполняются в текстовом режиме при старте компьютера. Обычно это красный текст на чёрном фоне, в котором в общем нет ничего нового, с требованием оплатить штраф за просмотр гей-порно, детского порно и видеоматериалов, содержащих насилие.

2 Trojan.Encoder.XXX - шифрование

"Добрый мишка Винни Пух хочет немножечко меда но злые кусачие пчелки не дают мишке мед поэтому он пришел и заблокировал злым пчелкам файлы DOC DOCX JPG JPEG и остальные офисные файлы если злые пчелки хотят свои файлы обратно они должны написать на эту: vinni_pux@yahoo.com почту и сказать эти буквы: bsn эти буквы очень важны и без них мишке будет трудно вернуть пчелкам их файлы :"

3 CryptoLocker, WannaCry, NotPetya - уничтожение

Используют все известные и новые способы проникновения на компьютер пользователя или в сеть (уязвимости ПО, социальная инженерия, поддельные сайты, зараженное ПО)
WannaCry – только EthernalBlue
NotPetya – EthernalBlue, Mimikatz, WMI, PsExec

Компания MAERSK – потеряли 150 контроллеров домена, 4000 серверов, только случайно копия одного DC осталась в Гане

#CODEIB


Новые вирусы и атаки будут
еще лучше технически
подготовлены,
100% защиты нет
#CODEIB

МЕТОДЫ ЗАЩИТЫ

ОРГАНИЗАЦИОННЫЕ

ПРОГРАММНЫЕ

ПРОГРАММНО-АППАРАТНЫЕ

ЧТО ЗАЩИЩАЕМ

ОДИНОЧНЫЙ КОМПЬЮТЕР

СЕТЬ БЕЗ ДОМЕНА

СЕТЬ С ДОМЕНОМ

ОРГАНИЗАЦИОННЫЕ

Написать инструкцию по информационной безопасности:

описать возможные опасные ситуации, методы социальной инженерии, которыми пользуются взломщики и мошенники:

- внезапные письма от госорганов с различными требованиями
- выигрыши призов
- письма с просьбой что-то срочно сделать или посмотреть (вложение или ссылку)
- найденные «флешки» могут быть целенаправленно подброшены

Пример подобной инструкции можно посмотреть здесь:

http://sergiuz-it.blogspot.com/2017/06/blog-post.html

Написать инструкцию пользователя компьютера:

Описать, что можно и что запрещается делать на рабочем компьютере, например:

- Использовать интернет, приложения или электронную почту в личных целях
- Использовать на работе личные флешки
- ответственность за утерю данных на компьютере несет пользователь, чтобы все рабочие данные хранили на сервере (только если есть файловый сервер)
- Запретить запускать приложения, скачанные из интернета или принесенные (portable-версии)

Написать политику по информационной безопасности:

Прописать максимальное количество ограничивающих действий для пользователя и ответственность:

- Пароль пользователю выдается и меняется через определенный срок
- Запретить хранить свой пароль на стикере около компьютера на видном месте
- Если носитель с паролем утерян (листок, фото на телефоне) – незамедлительно сообщать администратору
- Передавать свой пароль другим сотрудникам или посторонним лицам
- Использовать рабочий пароль в других системах
- Прописать политику работы с электронной почты в зависимости от должности (сотруднику юр.отдела запрещено читать письма с предложениями от контрагентов и соотвественно сотруднику отдела закупа или продаж – открывать письма от госорганов)

ПРОГРАММНЫЕ

БЕСПЛАТНЫЕ

1. Ставить ОС на диск с GPT (есть ограничения), желательно последние версии.
2. Защитить MBR (Cisco MBR Filter)
3. Устанавливать критические обновления Windows и программ (для крупных сетей с обязательным предварительным тестированием)
4. Никогда не работать под учетной записью пользователя с правами администратора
5. Отключить учетную запись администратора созданную по умолчанию.
6. Создать свою уникальную учетную запись пользователя с правами администратора – пароль сделать уникальным (создается скрипт, прячем в папку с ограниченным доступом, отрабатывает по событию, например при загрузке, берем любую переменную с компьютера + некий префикс) – Комп1Пароль, Комп2Пароль. Таким образом, зная префикс, администратор на любой машине может управлять ей полностью, если даже будет скомпрометирован пароль локального администратора на одной машине, то на других он уже не подойдет.
7. Ограничение запуска вложений с почтовых клиентов, ограничение отображения HTML вложений в почтовых клиентах
8. Отключение папок общего доступа на компьютерах, ограничение доступа в общие папки на сервере по группам доступа, отключение сетевых дисков на компьютерах
9. Запрет запуска PsExec (удаленное управление команд)
10. Ограничить logon type для привилегированных пользователей на компьютерах и серверах (ограничить сетевой вход, пакетный, вход в качестве службы, локальный, RDP) – тем самым получив пароль привилегированного пользователя – вирус не сможет захватить машину
11. Отключение передачи и хранения NTLMv1 хешей в домене
12. Отключить протокол SMB v1 на устройствах и в сети
13. Развести рабочие компьютеры, сервера, устройства по разным подсетям.
14. Заблокировать локальный трафик с других ПК пользователей
15. Использовать встроенный файрвол или бесплатные аналоги (Outpost, Comodo) – сложность в настройке
16. Исключить интерактивный выход в интернет с серверов, оставить только служебный трафик с ограничениями (при заражении вирус не сможет закачать дополнительное ПО)
17. Использовать для администрирования отдельный ПК или виртуальную машину
18. Отключить интернет, там где он не нужен (например не указывая адрес шлюза)

ПРОГРАММНЫЕ

APP LOCKER

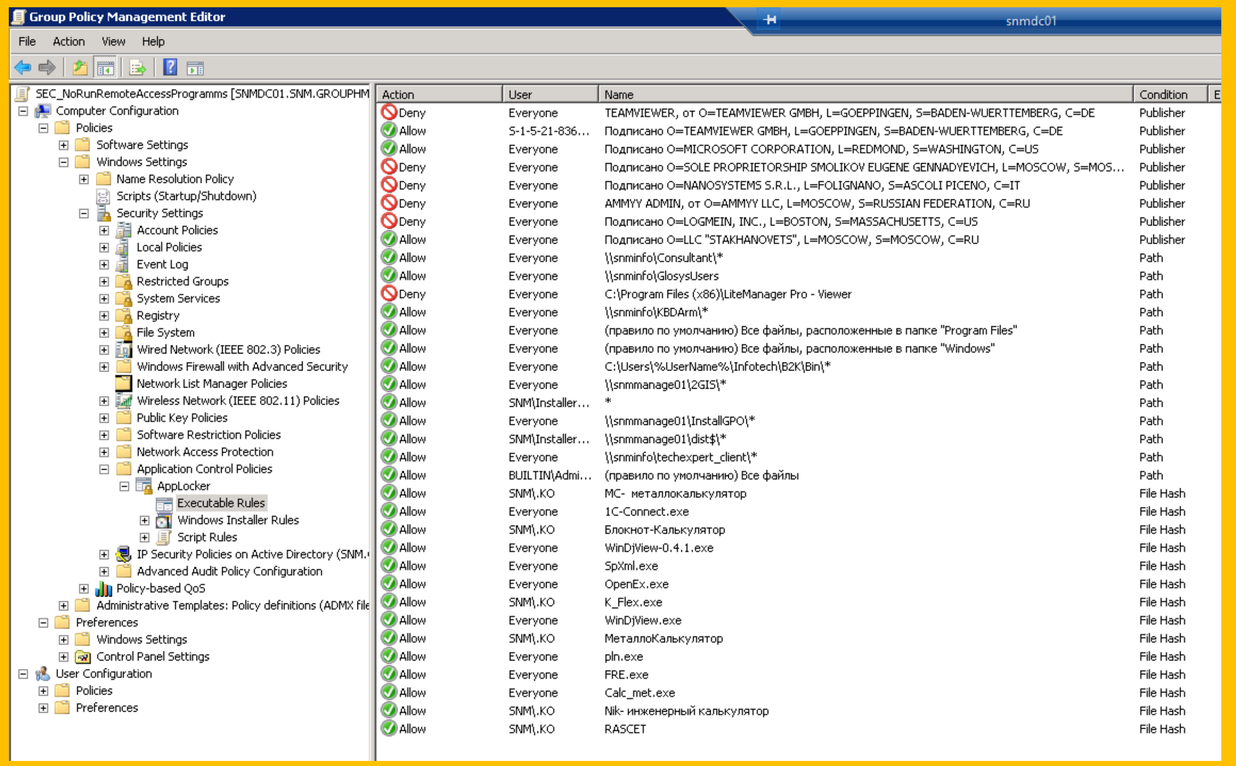
БЕСПЛАТНЫЕ

1. **Работает только в корпоративной версии, позволяет настроить ограничения запуска приложений по пути, хэшу файла или издателю.**

2. **У нас разрешено запускать пользователю приложения только из папки Program files и Windows, но у пользователя нет прав записывать в эти папки, таким образом даже portable версии не получится запустить с правами пользователя компьютера.**

3. **Для старых и других версий есть технология – Software Restriction Police, но она уже не поддерживается в релизе Windows 10 1809**

4. **Использовать «Защитник Windows»**



Принцип работы

Потенциально нежелательные приложения блокируются, когда пользователь пытается загрузить или установить обнаруженный файл и если файл соответствует одному из следующих условий:
файл проверяется из браузера;
файл находится в папке "**загрузки**";
файл находится в папке "**temp**";
Файл находится на рабочем столе пользователя
файл не соответствует одному из этих условий и не находится в папке *%programfiles%*, *%appdata%* или *%windows%*;
файл помещается в карантин, поэтому не запускается.
При обнаружении потенциально нежелательного приложения на конечной точке конечная точка отображает пользователю уведомление (если уведомления не были отключены) в таком же формате, как и при обнаружении обычных угроз (в начале уведомления отображается "PUA").
Они также будут отображаться в обычном списке карантина в приложении безопасности Windows

ПРОГРАММНЫЕ

LAPS

БЕСПЛАТНЫЕ

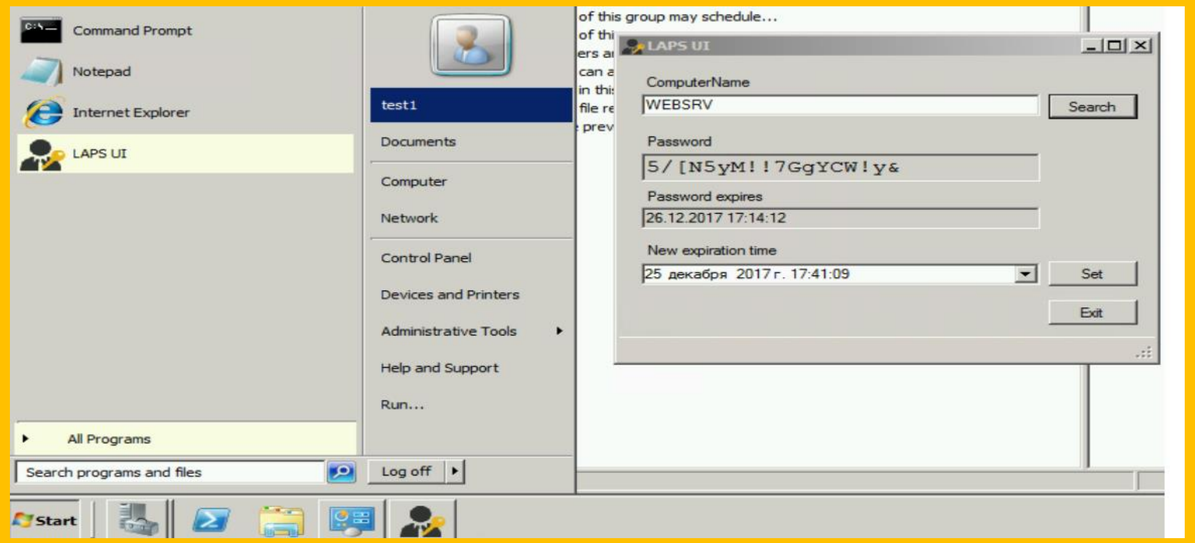
1. **Local Administrator Password Solution (LAPS) позволяет организовать решение по централизованному контролю и управлению паролями локальных администраторов на всех компьютерах домена с хранением информации о пароле непосредственно в объектах Active Directory типа Computer.**

2. **Функционал LAPS основан на технологии Group Policy Client Side Extension (CSE) и заключается в генерации и установки уникального пароля локального администратора на каждом компьютере домена. Пароль автоматически меняется через определенный интервал времени. Значение текущего пароля хранится в конфиденциальном атрибуте учетных записей компьютеров в Active Directory, доступ на просмотр содержимого атрибута регулируется группами безопасности AD.**

3. **Сложна в настройке и требует хороших знаний AD**

4. **Неудобно работать администраторам, т.к. если настроить смену пароля каждый день, или сложные пароли то приходится обращаться каждый раз**

5. **Если потеряется контроллер домена, то восстанавливать доступ к рабочим компьютерам придется только с загрузочного носителя.**



ПРОГРАММНЫЕ

ПЛАТНЫЕ

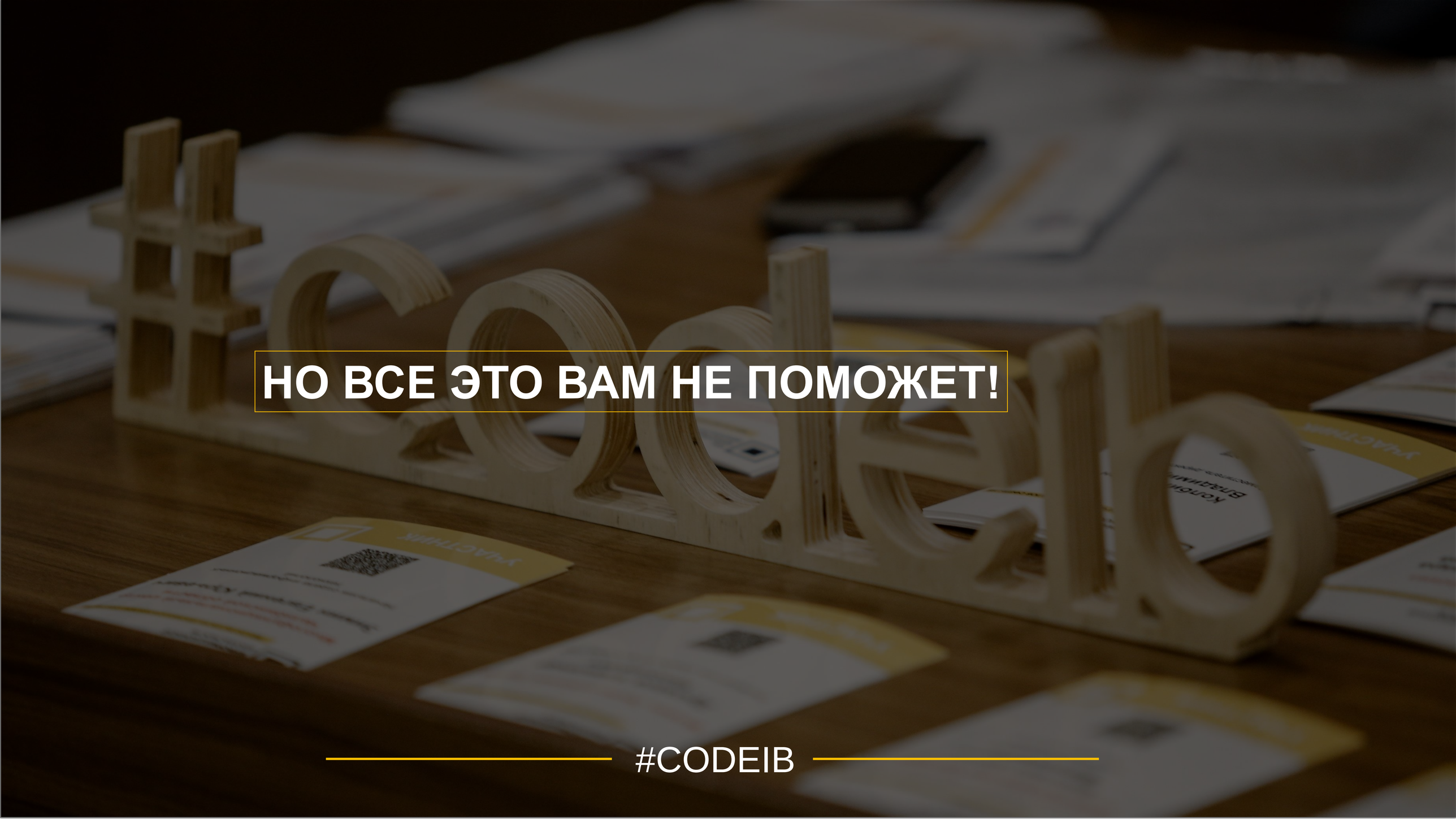
1. **Установить Acronis True Image (для небольших компаний или домашний пользователь)**
2. **Установка антивируса (выбор по религии) – использование белого списка программ, сканирование известных уязвимостей, проверка обновлений программного обеспечения**
3. **Установка программного межсетевого экрана (выбор зависит от сотрудника, умеющего работать с ним, от стоимости)**
4. **Почтовый антивирус**
5. **Система фильтрации почтового трафика, весь ваш трафик уходит на сервис по фильтрации, а потом возвращается обратно. Система требует настройки и корректировки. (Яндекс, Antispam Post, Спаморез)**
6. **Системы мониторинга (PTRG) – Zabbix, Nagios – бесплатные альтернативы (можно настроить сенсоры на загрузку процессора, диска, выросший трафик)**
7. **Сервисы для тестирования персонала (Антифишинг)**
8. **Использование SIEM систем, создание или аренда SOC**

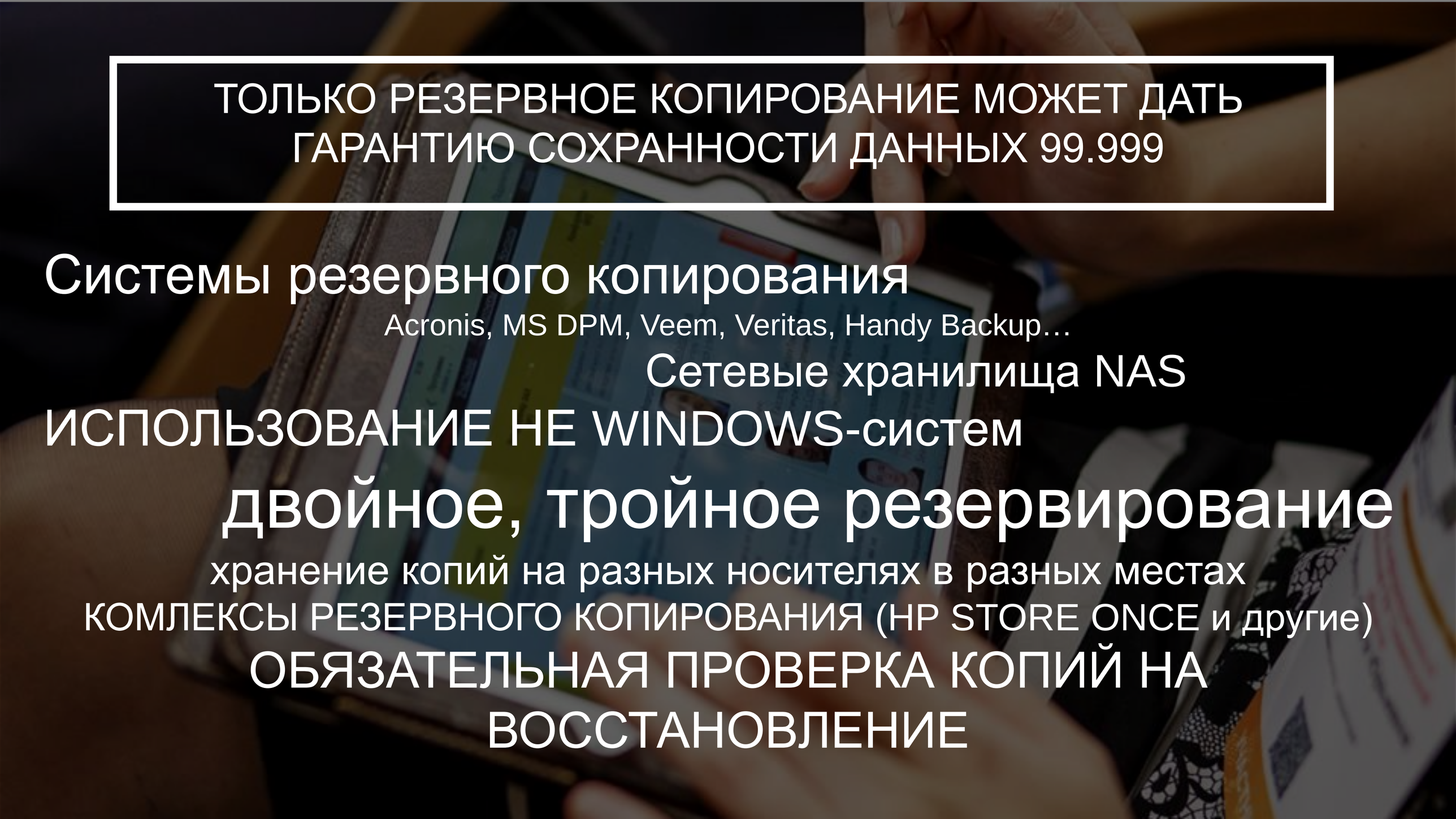
АППАРАТНЫЕ

1. **Использование двухфакторной аутентификации (JaCarta) – для привилегированных пользователей обязательно использовать.**
2. **Системы IDS, IPS, NGFW – выбор большой, вендоры дают все железки на тесты, помогают с настройкой.**
3. **Использование «песочниц» – программных или аппаратных**
4. **Выделенные сервера или системы резервного копирования**

ОБУЧЕНИЕ СОТРУДНИКОВ

1. **Литература и курсы для администраторов**
2. **Участие в профильных конференциях**
3. **Мотивация на отсутствие инцидентов, как администраторы, так и пользователи**
4. **Ежемесячные «напоминалки» пользователям о внимательности и примеры возможных атакующих действий (заодно освежаете инструкцию по информационной безопасности)**


НО ВСЕ ЭТО ВАМ НЕ ПОМОЖЕТ!
#CODEIB



ТОЛЬКО РЕЗЕРВНОЕ КОПИРОВАНИЕ МОЖЕТ ДАТЬ ГАРАНТИЮ СОХРАННОСТИ ДАННЫХ 99.999

Системы резервного копирования

Acronis, MS DPM, Veem, Veritas, Handy Backup…

Сетевые хранилища NAS

ИСПОЛЬЗОВАНИЕ НЕ WINDOWS-систем

двойное, тройное резервирование

хранение копий на разных носителях в разных местах

КОМЛЕКСЫ РЕЗЕРВНОГО КОПИРОВАНИЯ (HP STORE ONCE и другие)

ОБЯЗАТЕЛЬНАЯ ПРОВЕРКА КОПИЙ НА ВОССТАНОВЛЕНИЕ

СРК АО «СИБНЕФТЕМАШ»

1. **Acronis BackUp – для резервирования виртуальных машин на сервере виртуализации (27 штук) – резервируются каждый день, храним на СХД, на выделенном томе 30 дней.**
2. **Microsoft DMP на хранилище HP Store Once —System State контроллеров домена и остальных серверов, резервируются ежедневно, храним 14 дней**
3. **Microsoft DMP на хранилище HP Store Once – базы данных exchange ~~пользователей~~, резервируются каждый день, храним 30 дней**
4. **Microsoft DMP на хранилище HP Store Once – данные файлового сервера, резервируются два раза в день, храним 31 дней**
5. **Microsoft DMP на хранилище HP Store Once – базы данных SQL, резервируются каждый день, храним 30 дней**
6. **Ручное сохранение не внешний носитель БД MS DPM**
7. **Встроенные средства резервирования MS SQL, полный бэкап – раз в сутки, храним 30 дней, инкрементные каждые 30 минут, храним 1 сутки, месячные архивы храним постоянно.**
8. **Автоматические бэкапы средствами систем (Perco, Компас, Битрикс)**

БЛИЖАЙШИЕ ПЛАНЫ

1. **Установка и запуск новой системы StoreOnce + DPM**
2. **Перенос одной из систем в другое помещение + подключение к ней ленточного накопителя**
3. **Приобретение недорого NAS на unix – для хранения образов серверов и ежедневных архивов MS SQL**
4. **Настройка мониторинга создания резервных копий в одном месте (сейчас только оповещения на почту, их уже два десятка и легко можно какое-то пропустить - нужна визуализация)**
5. **Ежемесячное тестирование архивов на восстановление**

СПАСИБО ЗА ВНИМАНИЕ!

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

01 ноября 2018 г.
г. Тюмень

#CODEIB

ЗАЩИТА ОТ ВИРУСОВ В СРЕДЕ WINDOWS

ПРОГРАММНЫЕ РЕШЕНИЯ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ

СЕРГЕЙ ЩЕРБАКОВ
АО «СИБНЕФТЕМАШ»

ТЕЛЕФОН: +7 (922) 477-00-27
EMAIL: sherbakov@sibneftemash.ru