КОМИТЕТ ПО НАУКЕ И ВЫСШЕЙ ШКОЛЕ
Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Санкт-Петербургский технический колледж управления и коммерции»

ПРОЕКТ

По предмету: Антивирусная безопасность

Подготовил студень гр.9КС-41
Лебедев Серафим
Руководитель проекта: Ануров А. Д.

Санкт-Петербург, 2021

- ***Предмет:*** Современное антивирусного ПО для обеспечения безопасности в компании
- ***Задачи:***
- Изучить литературу по теме исследования.
- Описать программные продукты, используемые в России.
- Проанализировать причины использования того или другого вида антивируса.
- Предоставить инструкцию по обеспечению безопасности при использовании антивирусного по (для сотрудников)
- ***Методы исследования:***
- Анализ
- Систематизация
- Сравнение и обобщение.

Непосредственный процесс разработки Концепции антивирусной безопасности предусматривает выполнение следующих функциональных задач:

- проведение анализа угроз антивирусной безопасности, которым может быть подвержена организация. Для этого в состав Концепции включается модель угроз безопасности, позволяющая описать характеристики тех вирусных атак, от которых должна быть защищена АС компании;
- проведение оценки текущего состояния антивирусной безопасности предприятия на основе имеющейся информации о структуре АС, а также оценка установленных средств защиты;
- разработка концептуальных подходов к защите типовых объектов автоматизации предприятия от возможных вирусных угроз;
- определение стратегии создания, эксплуатации и развития комплексной системы антивирусной безопасности;
- формирование плана первоочередных и долгосрочных мер по реализации положений Концепции.

Стабильность и надежность работы

- Этот параметр, без сомнения, является определяющим — даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на вашем компьютере, если в результате какого-либо сбоя в работе программы процесс проверки компьютера не пройдет до конца. Тогда всегда есть вероятность того, что какие-то зараженные файлы остались незамеченными.

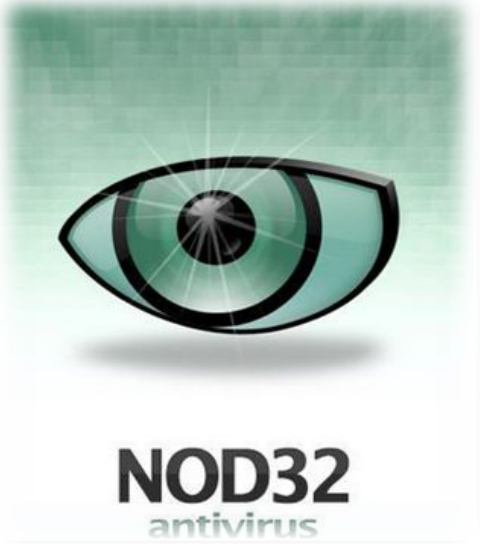
Скорость работы программы

- Наличие дополнительных возможностей типа алгоритмов определения даже неизвестных программе вирусов (эвристическое сканирование). Сюда же следует отнести возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является также процент ложных срабатываний программы (ошибочное определение вируса в “чистом” файле).

Многоплатформенность

- Наличие версий программы под различные операционные системы. Конечно, если антивирус используется только дома, на одном компьютере, то этот параметр не имеет большого значения. Но вот антивирус для крупной организации просто обязан поддерживать все распространенные операционные системы. Кроме того, при работе в сети немаловажным является наличие серверных функций, предназначенных для административной работы, а также возможность работы с различными видами серверов.

Топ 3 Антивирусных программ



NOD32 — антивирусный пакет, выпускаемый словацкой фирмой Eset. Возник в конце 1998 года. Название изначально расшифровывалось как Nemocnica na Okraji Disku («Больница на краю диска», перефразировавшие название популярного тогда в Чехословакии телесериала «Больница на окраине города»).

- защита всех устройств предприятия от любых угроз;
- безопасность использования мобильных устройств. Теперь вся информация, хранящаяся на телефонах и планшетах, находится под защитой антивируса;
- защита файловых серверов без снижения производительности их работы;
- безопасное использование корпоративной почты, мощный спам-фильтр, антишпион и другие способы защиты почтовых серверов компании;
- обеспечение безопасности HTTP- и FTP шлюзов;
- гибкое централизованное управление безопасностью.

Антивирус Касперского

Антиви́рус Каспе́рского (англ. *Kaspersky Antivirus, KAV*) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также от неизвестных компоненту «файловый антивирус» угроз с помощью проективной защиты, включающей компонент HIPS (только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»).

- Защита от вирусов, троянских программ и червей
- Защита от шпионских и рекламных программ
- Проверка файлов в автоматическом режиме и по требованию
- Проверка почтовых сообщений (для любых почтовых клиентов)
- Проверка интернет-трафика (для любых интернет-браузеров)
- Защита интернет-пейджеров (ICQ, MSN)
- Мониторинг активности (собирает данные о действиях программ на компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты).

- Защита от вирусов, червей и другого вредоносного ПО[3].
- DeepGuard — защита от неизвестных вирусов.
- F-Secure Anti-Virus выводит на экран гаджет, сообщающий о текущем состоянии защиты.

F-Secure Anti-Virus — антивирусная программа финской компании F-Secure. Антивирус сочетает в себе как сигнатурное обнаружение с помощью ядра Avira (BitDefender до 1 февраля 2019 года), так и собственные разработки компании, нацеленные на обнаружение неизвестных вирусов[1][2]. До версии 2010 года использовалось ядро от Лаборатории Касперского.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами сотрудники обязаны:

- Приостановить работу;
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- Провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов ОА);
- В случае обнаружения нового вируса, не поддающегося лечению 'применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске в ОА для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку;
- По факту обнаружения зараженных вирусом файлов составить служебную записку в отдел обеспечения безопасности информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

СПАСИБО ЗА ВНИМАНИЕ!!!!