О ПРИМЕНЕНИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

НАЧАЛЬНИК ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ЦЕНТРА ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ИНСТИТУТА РАЗВИТИЯ ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

КРЯЖЕВСКИХ АЛЕКСАНДР ВЛАДИМИРОВИЧ

Общее определение и цель

- Антивирусная защита — это комплекс технологий и программных решений, направленных на обнаружение, блокировку, предотвращение проникновения и удаление вредоносных программ (вирусов, троянов, шпионского ПО, программ-вымогателей и других угроз) с компьютеров, мобильных устройств и в информационных системах.

- Её основная цель — защитить устройства, данные и системы от кибератак, которые могут привести к утечке информации, финансовым потерям или нарушению работы.

Администраторы и пользователи

- Выполнение обязанностей по администрированию средств антивирусной защиты в Организации возлагается на администратора информационной безопасности.
- Пользователь обязан изучить руководящие инструкции по антивирусной защите и ознакомиться с необходимостью несения ответственности за выполнение его требований под подпись.

Порядок учёта, проверок и обновлений баз сигнатур

- Должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в Организации
- Централизованное управление
- Антивирусная проверка должна осуществляться для следующих объектов: файлов загрузки, системного и прикладного ПО, по каналам связи, подключение иных носителей, устанавливаемое ПО и т.д.
- Обновление баз данных вирусных сигнатур должно производится автоматический на ежедневной основе



Действия при обнаружении

5

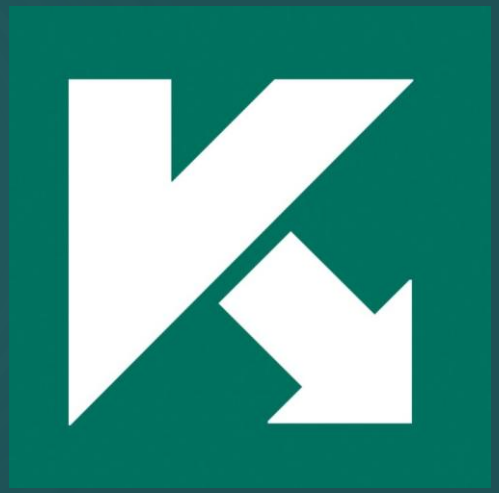
- Приостановить все работы на рабочем месте
- Сообщить непосредственному руководителю и администратору информационной безопасности в Организации о факте обнаружения программного вируса
- Принять по согласованию с администратором информационной безопасности меры по изоляции зараженного рабочего места от локальной сети Организации и информационной-телекоммуникационной сети «Интернет»,
- Локализации и удалению программного вируса с использованием средств антивирусной защиты информации

Антивирусное ПО на практике

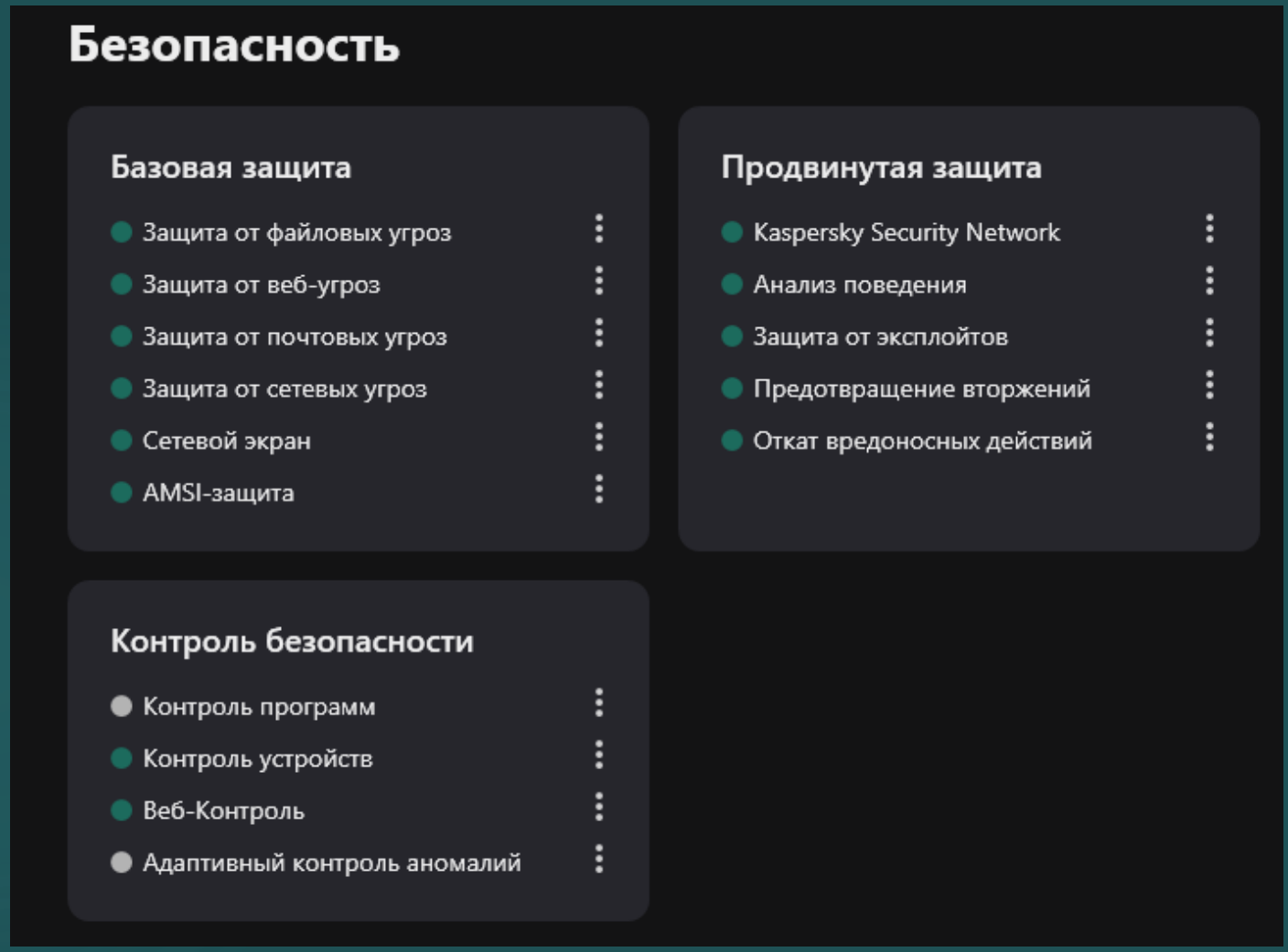
- Импортозамещение
- Цели и задачи
- Технологичность и эффективность
- Стоимость лицензирования

Антивирусное ПО на практике

- Kaspersky Endpoint Security (KES), (обычная версия 14.1, серт. версия ФСТЭК/ФСБ 12.12)
- Dr.WEB, (обычная версия 12.4, серт. версия ФСТЭК 12.4)



Kaspersky Endpoint Security (KES)



Политики

- Пароль администратора на изменение конфигурации
- Расписание задач поиска нежелательного ПО и источник обновлений вирусных сигнатур
- Белые и чёрные списки веб-доступа
- Контроль съёмных устройств
- Контроль приложений
- Исключения

Благодарю за внимание!

КРЯЖЕВСКИХ АЛЕКСАНДР ВЛАДИМИРОВИЧ

ТЕЛЕФОН:

8(8332) 25-54-42 (ДОБ. 227)

АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ:

AV.KRYAZHEVSKIH@KIROVIPK.RU