

Рекомендации

Основные меры кибербезопасности3

Специфические меры безопасности11

Основные меры кибербезопасности

Базовые меры и практики обеспечения безопасности, которые помогают защититься от различных киберугроз на всех этапах атаки.

1. Защитите узлы ИТ- и технологической сети с помощью подходящего современного решения.

- Хосты технологических сетей: для защиты рекомендуем использовать специализированное решение, такое как [Kaspersky Industrial CyberSecurity for Nodes](#), на инженерных рабочих станциях, системах человеко-машинного интерфейса и серверах технологической сети.
- Смежные с технологической сетью хосты в демилитаризованной зоне и ИТ-сегменте: для защиты можно использовать корпоративное решение, например [Kaspersky Security для бизнеса](#).

Эти решения при правильной настройке надежно защищают от большинства актуальных угроз – блокируют обращение ко вредоносным ресурсам, обнаруживают и блокируют вредоносное программное обеспечение – скрипты, исполняемые файлы, вредоносные документы, анализируя, в том числе и поведение приложений, позволяют ограничить исполняемую среду списком разрешенных приложений и динамических библиотек и подключать только разрешенное оборудование и т. д.

2. Усиьте сегментацию сети и ограничьте доступ в интернет из технологической сети.

- Разделите сети различных предприятий (а также различных подразделений) на отдельные сегменты, используя технологию VLAN.
- Ограничьте передачу данных между сегментами сети до минимально необходимого набора портов и протоколов, требуемых для обеспечения рабочих процессов организации.
- Обеспечьте строгое применение ACL (Access Control List) – списков управления доступом. Используйте межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), чтобы ограничить исходящие соединения из технологической сети разрешенными адресатами. Установите расписание, подтверждайте и документируйте все необходимые исключения в соответствии с ним.
- Осуществляйте мониторинг технологических сетей с помощью решений для пассивного мониторинга, например, [Kaspersky Industrial CyberSecurity for Networks](#), для обнаружения и своевременного

оповещения о несанкционированном интернет- и VPN-трафике и прочих попытках нарушения политик сетевого доступа.

- Заблокируйте неразрешенные VPN/hotspot-приложения, отключите модемы (особенно неавторизованные USB-устройства) и изолируйте узлы, нарушающие политики безопасности, например, с помощью решения [Kaspersky Industrial CyberSecurity](#).
- Там, где требуется ограниченный доступ в интернет, обеспечьте его через защищенный интернет-шлюз, например, с помощью [Kaspersky Security for Internet Gateway](#), для централизованной фильтрации URL и применения политик безопасности.
- Если необходим удаленный доступ к системам в других сегментах сети, используйте концепцию демилитаризованной зоны для организации взаимодействия между сегментами и осуществляйте удаленный доступ через терминальные серверы.

3. Установите последние версии операционных систем и прикладного ПО.

- Обновите Microsoft Windows и Unix-подобные операционные системы до версий, поддерживаемых их производителями.
- Установите актуальные обновления безопасности (патчи) для ОС и приложений.
- Особое внимание уделите обновлению гипервизоров.
- Обновите прикладное программное обеспечение, включая Microsoft Office, веб-браузеры. Установите все виды обновлений: накопительные (CU), сервисные пакеты (SP) и обновления безопасности (патчи).
- Особое внимание уделите сервисам, доступным из интернета.

4. Реализуйте многофакторную аутентификацию.

- Включите двухфакторную аутентификацию для входа в консоли администрирования и веб-интерфейсы защитных решений. В Kaspersky Security Center, например, это можно настроить [вручную](#).
- Реализуйте двухфакторную аутентификацию для авторизации (по RDP, SSH и другим протоколам) на системах, содержащих конфиденциальные данные, а также на критически важных системах ИТ- и технологической инфраструктур организации, таких как контроллеры доменов и серверы SCADA.
- Используйте двухфакторную аутентификацию для входа в сервисы с доступом из интернета, такие как веб-интерфейс электронной почты.

5. Повысьте требования к паролям для операционных систем и сервисов.

- Обязайте сотрудников использовать разные пароли для различных доменов, сервисов и систем.
- Установите в политиках сервисов и систем следующие требования к сложности паролей:
 - Длина пароля: не менее 12 символов для непривилегированных учетных записей и не менее 16 символов для привилегированных.
 - Пароль должен содержать заглавные и строчные буквы, цифры и специальные символы:
(! @ # \$ % ^ & * () - _ + = ~ [] { } | \ ; ' " < > , . ? /)
 - Пароль не должен содержать словарных слов или персональных данных пользователя, которые могут быть использованы для его подбора, таких как имя или фамилия, номер телефона, памятные даты (дни рождения и т. д.).
 - Пароль не должен содержать символы, последовательно расположенные на клавиатуре (12345678, QWERTY и т. д.), а также распространенные сокращения и шаблонные слова (USER, TEST, ADMIN и др.).
- Срок действия пароля — не более 90 дней.

6. Запретите хранение и передачу паролей и прочих секретных данных (закрытых ключей, сертификатов и токенов доступа) в открытом виде.

- Для хранения и передачи паролей, ключей, сертификатов используйте специализированные программы — менеджеры паролей.
- При необходимости передачи мастер-пароля к базам паролей используйте второй канал связи, например, SMS или чат с сквозным шифрованием в мессенджерах.
- Удаляйте сообщения, содержащие секретные фразы (пароли, ключи и т. д.).
- Регулярно проверяйте рабочие компьютеры пользователей и общие папки на наличие файлов с паролями в открытом виде по имени файла и содержимому.
- Регулярно проверяйте исходный код систем собственной разработки, а также файлов конфигурации ИТ- и технологических систем.

7. Используйте строгие политики безопасности домена.

- Ограничьте использование учетных записей с правами локального администратора и администратора домена.
- Потребуйте от администраторов использовать привилегированные учетные записи только в тех случаях, когда без этого невозможно выполнение их рабочих задач.
- Используйте выделенные учетные записи для администрирования разных групп систем, например, серверов баз данных, почтовых серверов.
- Ограничьте пользовательский доступ к системам. Проверьте политики в Active Directory: пользователи должны иметь доступ только к тем системам, которые необходимы им для выполнения их служебных обязанностей.
- Внедрите практику, при которой доменные учетные записи обычных пользователей не имеют прав локального администратора. Это поможет снизить риск повышения привилегий в случае компрометации таких учетных записей.

8. Обеспечьте создание автономных и неизменяемых резервных копий критически важных технологических систем и проводите тестовые восстановления.

- Храните резервные копии на отдельном сервере, не входящем в домен. Наделите правами на удаление/изменение копий выделенную учетную запись, также не входящую в домен.
- Увеличьте частоту создания резервных копий, чтобы свести к минимуму потери данных.
- Храните не менее трех копий, причем как минимум одну из них – на отдельном автономном устройстве.
- Используйте RAID-массивы на серверах, где хранятся резервные копии, для повышения отказоустойчивости.

Эти меры особенно важны для снижения риска тяжелых последствий атак вымогателей.

9. Настройте защитные решения.

- Сведите к минимуму количество исключений в политиках защитных решений. По возможности не задавайте исключения с помощью универсальных масок (*), вместо этого заменяйте их исключениями для конкретных файлов или расширений.
- Настройте защитные решения на блокировку запуска утилит удаленного администрирования (за исключением используемых

администраторами). Продукты [Kaspersky Industrial CyberSecurity](#) умеют обнаруживать средства удаленного администрирования, используемые в технологической среде (поиск событий «Выполнение средств удаленного администрирования (RAT)»).

- Убедитесь, что все компоненты защитных решений активны на всех системах, а действующие политики не позволяют отключать защиту и завершать работу защитных решений или удалять их без ввода пароля администратора.
- Убедитесь, что защитные решения получают актуальные сведения об угрозах из Kaspersky Security Network для тех групп систем, где использование облачных сервисов не запрещено нормативными актами.
- Убедитесь, что все устройства распределены по группам (отсутствуют устройства в группе «Неизвестные устройства»), лицензионные ключи защитных решений установлены на всех устройствах, для всех групп созданы задачи периодической проверки.
- Перенесите сервисы, связанные с обеспечением информационной безопасности организации, в отдельный сегмент сети, а по возможности — в отдельный домен.
- Для настройки защитных решений Kaspersky следуйте [Руководству по усилению защиты](#).

10. Минимизируйте поверхность атаки на конечные узлы технологической сети.

- Отключите USB-порты в настройках операционной системы и BIOS/UEFI. Сделайте исключения только для авторизованных устройств и обеспечьте защиту от атак BadUSB, например, с помощью модуля «Контроль устройств» решения [Kaspersky Industrial CyberSecurity for Nodes](#).
- Для всех подключаемых носителей используйте выделенные пункты передачи с двойным контролем (правило двух лиц), а также журналирование с защитой журналов от несанкционированного изменения и удаления, выполняйте сканирование носителя на контролируемой станции до ввода файлов внутрь технологической сети, сохраняйте журналы всех операций передачи, сканирования и допуска, исключения допускайте только при подтверждении двумя ответственными сотрудниками.
- Разрешите запуск в технологической сети только доверенных приложений. Для контроля запуска программ можно использовать модуль «Контроль запуска программ» решения [Kaspersky Industrial CyberSecurity for Nodes](#).

- Используйте мониторинг сети для обнаружения несоответствующей сетевой активности и аномалий вроде подключения к подозрительным серверам. Для этого можно использовать специализированное решение для обеспечения кибербезопасности, такое как [Kaspersky Industrial CyberSecurity for Networks](#).
- Настройте решение для защиты конечных точек таким образом, чтобы оно разрешало подключения только к авторизованным веб-ресурсам, например, используя функцию управления сетевым экраном в решении [Kaspersky Industrial CyberSecurity for Nodes](#) для создания правил списка разрешенных веб-серверов, или используя модуль «Веб-контроль» в [Kaspersky Industrial CyberSecurity for Linux Nodes](#).

11. Усиьте защиту электронной почты и настройте анализ сообщений до доставки, чтобы снизить риск фишинговых атак.

- Настройте фильтрацию содержимого исходящей электронной почты и внедрите многоуровневую фильтрацию входящих почтовых сообщений.
- Усиьте защиту от спама и фишинга на интернет-шлюзе, чтобы блокировать вредоносные сообщения до их доставки, например, с помощью [Kaspersky Secure Mail Gateway](#).
- Проверяйте в песочнице потенциально опасные вложения до их доставки и помещайте на карантин на основании вердикта, например, с помощью [Kaspersky Anti Targeted Attack](#).
- Периодически выполняйте повторное сканирование почтовых ящиков/хранилищ для выявления отложенной активации фишинговых URL-адресов/URL с изменившейся репутацией, например, с помощью [Kaspersky Security for Mail Server](#), где есть функция повторной проверки писем после доставки.

12. Проведите обучение сотрудников.

- Проведите симуляцию фишинговых атак и объясните последствия загрузки/запуска файлов из непроверенных источников.
- Обучите сотрудников правилам безопасной работы в интернете, с электронной почтой и другими каналами связи.
- Для инженеров и операторов проведите [тренинг «Основы промышленной кибербезопасности»](#).
- Для специалистов по информационной безопасности проведите [тренинг «Цифровая криминалистика и расследование инцидентов в АСУ ТП»](#).

- Разработайте инструкции по реагированию на различные типы инцидентов, в этом поможет [услуга «Разработка руководства и обучение реагированию на инциденты»](#).

13. Разверните SIEM-систему с установленным релевантным набором правил корреляции, например, [Kaspersky Unified Monitoring and Analysis Platform](#), и дополните его следующими правилами.

- Подключение нового USB-накопителя к узлу в технологической сети.
- Создание запланированной задачи или элемента автозагрузки на конечном устройстве технологической сети.
- Вход в систему с использованием протоколов RDP или SSH в нерабочее время.
- Успешная авторизация пользователя с правами администратора на новой системе.
- Очистка журналов событий Windows или отключение служб журналирования.
- Обнаружение вредоносного ПО средствами защиты конечных узлов.
- Блокировка доступа к вредоносным веб-ресурсам защитными решениями.
- Использование несанкционированных средств удаленного администрирования (RAT).
- Создание новой службы в операционных системах Windows.
- Остановка служб или завершение (terminate, kill) процессов защитных решений.
- Появление скрытых пользователей в системе.
- Обнаружение событий запуска утилиты PSEXEC и аналогичных событий.
- Успешный вход через VPN в технологическую сеть из несанкционированной сети или без двухфакторной аутентификации.
- Попытка входа с использованием заблокированной или отключенной учетной записи.
- Блокировка учетной записи из-за многократного неверного ввода пароля.
- Появление нового пользователя в привилегированной группе, например, администратора домена.
- Попытки запуска неавторизованного приложения на конечном узле технологической сети при включенном режиме разрешенных списков.
- Попытки исходящих подключений из сегментов технологической сети в обход разрешенного прокси-сервера или NGFW.

- Попытки исходящих подключений из сегментов технологической сети к неизвестным внешним хостам при включенном режиме разрешенных списков.
- Массовые подключения к известным портам на нескольких системах (сканирование сети).
- Аномально большой объем исходящего трафика из сегментов технологической сети.
- Массовые DNS-запросы из сегментов технологической сети.
- Неавторизованные VPN-подключения из сегментов технологической сети, для которых использование VPN не разрешено.
- Обнаружение нового устройства в технологической сети решением [Kaspersky Industrial CyberSecurity for Networks](#).
- Обнаружение некорректных пакетов данных решением [Kaspersky Industrial CyberSecurity for Networks](#).

Специфические меры безопасности

Меры защиты и рекомендации, критически важные для противодействия отдельным типам киберугроз.

14. Внедрите специализированные решения для защиты от целевых атак (APT/хактивисты/ высокоорганизованные киберпреступники, использующие продвинутые шпионские программы и программы-вымогатели, а также техники Living off the land (LOTL)).

- Внедрите комплексное решение для обнаружения сложных угроз как на уровне конечных устройств, так и на уровне сети. Это решение должно уметь анализировать поведение с использованием песочницы, а также обладать функционалом реагирования на инциденты. Одним из таких решений является [Kaspersky Anti Targeted Attack](#).
- Используйте углубленный мониторинг поведения прикладных программ на конечных устройствах для оперативного выявления угроз. Для этого можно использовать [Kaspersky EDR Expert](#).
- Также можете делегировать задачу поиска, обнаружения и устранения угроз, направленных на вашу инфраструктуру, специалистам «Лаборатории Касперского», воспользовавшись услугой [Kaspersky Managed Detection and Response](#).
- Отслеживайте изменения в ландшафте угроз и корректируйте меры кибербезопасности, чтобы противостоять новым вызовам, используя релевантные источники информации об угрозах, в том числе комплекс сервисов [Kaspersky Threat Intelligence](#).
- Регулярно проверяйте, не были ли страницы входа в ваши сервисы, к которым есть удаленный доступ, изменены с внедрением вредоносного импланта и что только вы по-прежнему контролируете DNS-зону своей организации.
- Регулярно проверяйте, не скомпрометированы ли учетные записи сервисов, к которым есть удаленный доступ, с помощью специализированных сервисов мониторинга угроз, например, [Kaspersky Digital Footprint Intelligence](#).
- Снизьте риск атаки на цепочки поставок и доверенных партнеров – проверяйте критически важных вендоров и закрепляйте в контрактах минимальные требования безопасности к ним самими и их продуктам, ограничьте и сегментируйте доступ партнеров только к необходимым ресурсам, устанавливайте обновления только из официальных источников с обязательной проверкой цифровых подписей.

15. Меры против техники **BYOVD** (АПТ/хактивисты/высокоорганизованная киберпреступность).

- Регулярно проводите инвентаризацию драйверов, например, с помощью [Kaspersky Industrial CyberSecurity for Nodes](#), обновляйте или удаляйте устаревшие драйверы.
- Выявляйте злоупотребление драйверами: отслеживайте системную активность для фиксации попыток загрузки драйверов или отключения средств защиты с их помощью, используя решения класса EDR/XDR, например, [Kaspersky EDR Expert](#). При ограниченных внутренних возможностях используйте MDR-сервис, например, [Kaspersky Managed Detection and Response](#), для круглосуточного триажа и реагирования на инциденты.
- Используйте SIEM-систему со следующим правилом корреляции: установка нового драйвера в системе.

16. Защита виртуальных сред и специальные меры против атак на уровне гипервизора.

- Изолируйте и усильте защиту уровня управления гипервизором (используйте отдельную сеть для управления, выделенные учетные записи администратора, а также многофакторную аутентификацию и принцип минимальных привилегий).
- Ограничьте и отслеживайте доступ к виртуальным консолям и API.
- Создавайте неизменяемые/автономные резервные копии конфигураций гипервизора/образов виртуальных машин.
- Для эффективной защиты виртуальных машин в сопряженных с ОТ сегментах IT и DMZ (VDI, jump-серверы, historian-серверы и др.) используйте [Kaspersky Security для виртуальных сред Легкий агент](#).
- Для виртуальных машин, непосредственно задействованных в автоматизированном управлении технологическим процессом, отдавайте предпочтение [Kaspersky Industrial CyberSecurity for Nodes](#), а не универсальным решениям для защиты виртуальных сред.

17. Компенсирующие меры защиты для устаревших операционных систем.

- Размещайте устаревшие или снятые с поддержки операционные системы (например, FreeBSD, старые версии Windows) в строго контролируемых зонах, разрешайте только необходимые протоколы и взаимодействие с утвержденными узлами, отключите неиспользуемые службы; осуществляйте администрирование только через максимально защищенный jump-сервер.

- Если EDR не поддерживается, внедрите мониторинг сетевого уровня, например, [Kaspersky Industrial CyberSecurity for Networks](#), регулярно проверяйте целостность/логи и делайте упор на проверенные процедуры восстановления (золотые образы + резервные копии), а не на точечную установку исправлений.

18. Меры против техники DLL hijacking.

- Используйте защитные решения класса EDR/XDR, например, [Kaspersky EDR Expert](#), для обнаружения загрузки подозрительных библиотек DLL. Если внутренние ресурсы ограничены, используйте решение MDR, например, [Kaspersky Managed Detection and Response](#), которое обеспечивает триаж и реагирование на инциденты в режиме 24/7.
- Используйте функцию создания разрешенных списков защитных решений конечных устройств, например, «[Контроль запуска программ](#)» в Kaspersky Industrial CyberSecurity for Nodes и «[Контроль приложений](#)» в Kaspersky Endpoint Security for Windows, чтобы отслеживать и блокировать запуск исполняемых файлов и загрузку DLL, а также оперативно расследовать попытки запуска. Настройте отправку событий с высокой достоверностью в SIEM для корреляции и реагирования.
- Настройте, где это поддерживается ОС, безопасный режим поиска DLL (Safe DLL Search Mode).
- Запускайте приложения только из доверенных, защищенных каталогов установки, запретите выполнение из каталогов, доступных пользователям на запись.

19. Меры против вредоносных программ для AutoCAD.

- Запретите AutoCAD загружать скрипты или плагины из неутвержденных каталогов – разрешите загружать только подписанные вендором компоненты, используйте список разрешенных приложений и контролируйте подключаемые устройства. Для этого можно использовать, например, функции «[Контроль запуска программ](#)» и «[Контроль устройств](#)» решения Kaspersky Industrial CyberSecurity for Nodes.
- Проверяйте архивы и почтовые вложения, содержащие файлы AutoCAD, до их доставки; проверяйте в песочнице CAD-вложения в электронной почте и неизвестные объекты, например, с помощью [Kaspersky Anti Targeted Attack](#), помещайте на карантин на основании вердиктов песочницы.

- Сканируйте входящие CAD-файлы на пунктах передачи данных в OT-сегмент и на конечных устройствах перед открытием (например, с помощью [Kaspersky Industrial CyberSecurity for Nodes](#) на конечных устройствах технологических сетей и [Kaspersky Security для бизнеса](#) на смежных/почтовых шлюзах, где это применимо).
- Создавайте с установленной периодичностью автономные резервные копии CAD-репозиториях, проводите тестовые восстановления и фиксируйте результаты.
- Обновляйте программное обеспечение Autodesk, проверяйте хеши и в тестовой среде перед запуском в рабочую среду.
- Используйте SIEM-систему со специальными правилами корреляции:
 - Обнаружение файлов с расширениями DWG/DXF с вердиктом «вредоносный»/«подозрительный».
 - Запуск ранее неизвестного плагина в AutoCAD.
 - Создание или модификация каталогов автозагрузки AutoCAD или каталогов макросов.
 - Перемещение защитными решениями в карантин вложений электронной почты с расширениями DWG/DXF.
 - Доступ к файлам в CAD-репозиториях, за которым следуют неожиданные исходящие соединения.

20. Дополнительные меры против майнеров.

- Запретите доступ к известным майнинг-пулам на устройствах защиты периметра, таких как NGFW, и на смежных узлах. На узлах это можно сделать, например, с помощью функции «Веб-контроль» в [Kaspersky Endpoint Security для Windows](#), используя настройку веб-контроля для блокировки доменов и категорий веб-ресурсов, а также для мониторинга попыток доступа к ним.
- Усиьте меры защиты доступных извне сервисов в демилитаризованной и смежных зонах, проведите аудит активных служб и портов и отключите неиспользуемые, отслеживайте устойчивые аномалии в работе процессоров и сетевой активности, а также нетипичные исходящие соединения.
- Обнаруживайте и устраняйте майнеры на конечных устройствах технологической сети, например, с помощью [Kaspersky Industrial CyberSecurity for Nodes](#).
- Используйте SIEM-систему со специальными правилами корреляции (например, [Kaspersky Unified Monitoring and Analysis Platform](#)):
 - Устойчивая высокая загрузка процессора процессом с неподтвержденной репутацией.

- Подключения к известным майнинг-пулам или криптовалютным протоколам.

21. Дополнительные меры против программ-вымогателей.

- Внедрите строгие политики резервного копирования (см. «Создание автономных и неизменяемых резервных копий критически важных технологических систем и тестовые восстановления»).
- Внедрите меры защиты от целевых атак (см. «Внедрение специализированных решений для защиты от целенаправленных атак»).
- Внедрите меры защиты от атак, в которых используется техника BYOBD (см. «Меры против техники BYOVD»).
- Внедрите меры защиты от атак, в которых используется техника DLL hijacking (см. «Меры против техники DLL hijacking»).
- Внедрите защиту виртуальных сред (см. «Защита виртуальных сред и специальные меры против атак на уровне гипервизора»).
- Внедрите защиту устаревших операционных систем (см. «Компенсирующие меры защиты для устаревших операционных систем»).
- Используйте SIEM-систему с релевантными правилами корреляции (например, [Kaspersky Unified Monitoring and Analysis Platform](#)):
 - Новая групповая политика со скриптами входа или выхода из системы.
 - Появление новых процессов на нескольких устройствах.
 - Запуск инструментов или команд, связанных с удалением теневой или резервной копий (vssadmin delete shadows, wmic shadowcopy delete, wbadmin delete catalog и т. д.).
 - Массовые события удаления, изменения или переименования файлов на файловых ресурсах за короткий промежуток времени.
 - Массовые подключения по протоколу SMB.
 - Завершение процессов агентов резервного копирования, служб баз данных, веб-серверов и т. д.
 - Обнаружение команд удаления резервных копий/снэпшотов или вызовов API для управления снэпшотами в инфраструктуре резервного копирования.
 - Обнаружение массовой доставки исполняемых файлов или скриптов через SMB, PsExec или WinRM.
 - Нехарактерные действия по управлению гипервизором (новые роли администратора, подключение с новых IP-адресов, нетипичные вызовы API, массовая перезагрузка/выключение/переконфигурация виртуальных машин, массовое создание/удаление снэпшотов).

- Аномалии в зоне с устаревшими системами (открытие новых входящих путей, неожиданные исходящие соединения с устаревших хостов, повторяющиеся ошибки аутентификации, включение новых служб удаленного администрирования).

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com