Ландшафт угроз для компьютеров, используемых для инжиниринга и интеграции АСУ ТП. 2020

Ландшафт угроз для компьютеров, используемых для инжиниринга и интеграции АСУ ТП, в значительной степени зависит от среды, в которой они находятся, включая географическое расположение, возможность доступа к внешним сетям и службам и поведение пользователей.

Объект исследования

В этом исследовании мы провели анализ киберугроз, заблокированных на компьютерах, используемых для разработки, настройки и обслуживания оборудования и программного обеспечения АСУ ТП. В частности, на компьютерах под управлением ОС Windows, на которых установлено различное ПО для проектирования и интеграции АСУ ТП.

Окружение, в котором обычно находятся компьютеры, используемые для инжиниринга АСУ ТП, значительно отличается от окружения большинства компьютеров АСУ ТП. Ключевое отличие состоит в том, что компьютеры инженеров АСУ часто имеют прямое и непрямое подключение к различным системам управления производством, некоторые из которых могут даже принадлежать другим промышленным предприятиям. Компьютеры инженеров АСУ обычно имеют больше прав доступа и вместе с тем меньше ограничений (таких как контроль приложений, управление устройствами и т.д.), что значительно увеличивает поверхность атаки.

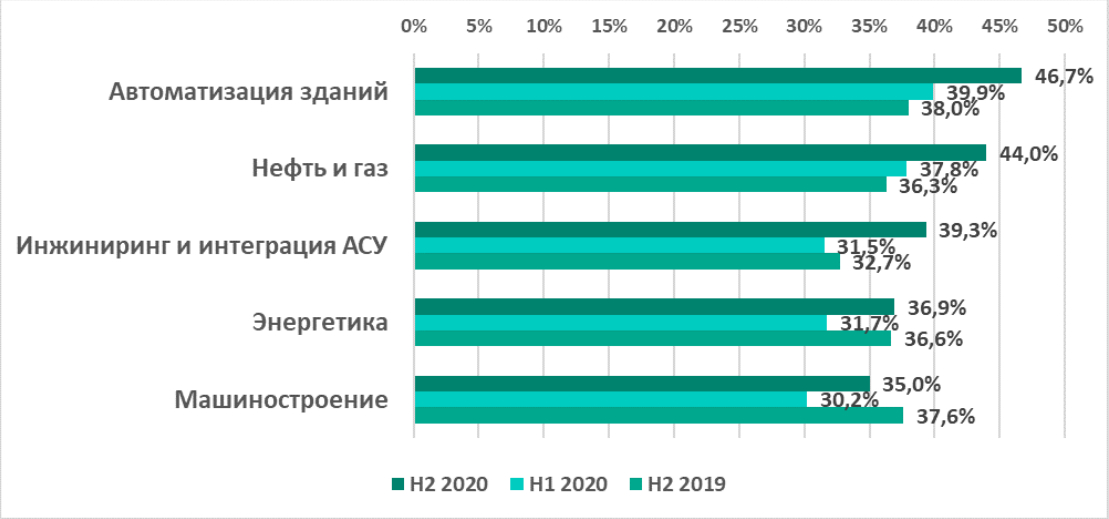
Большинство компьютеров инженеров АСУ обладают следующими недостатками с точки зрения информационной безопасности:

- позволяют устанавливать любое ПО;
- одновременно подключены к корпоративной сети и системам АСУ в технологической сети;
- имеют доступ в интернет, доступ к почтовым сервисам, сетевым папкам и мессенджерам.

В то же время мы заметили, что на компьютерах инженеров АСУ угрозы устраняются намного быстрее, чем на компьютерах АСУ. В типичной среде АСУ ТП компьютер может неоднократно подвергаться атаке одной и той же вредоносной программы из-за наличия в сети постоянного источника заражения, в то время как компьютеры инженеров АСУ значительно быстрее реагируют и справляются с угрозами.

Процент компьютеров, на которых было заблокировано вредоносное ПО

Во втором полугодии 2020 года продукты «Лаборатории Касперского» заблокировали вредоносное ПО на 39,3% компьютеров, используемых для проектирования и интеграции АСУ ТП, что значительно больше, чем в первом полугодии 2020 года (31,5%). За последние шесть месяцев 2020 года также увеличились доли в нескольких отраслях, включая автоматизацию зданий, автомобилестроение, энергетику и нефтегазовый сектор, хотя наибольший рост (7,8 п.п.) пришелся на сектор инжиниринга АСУ ТП.

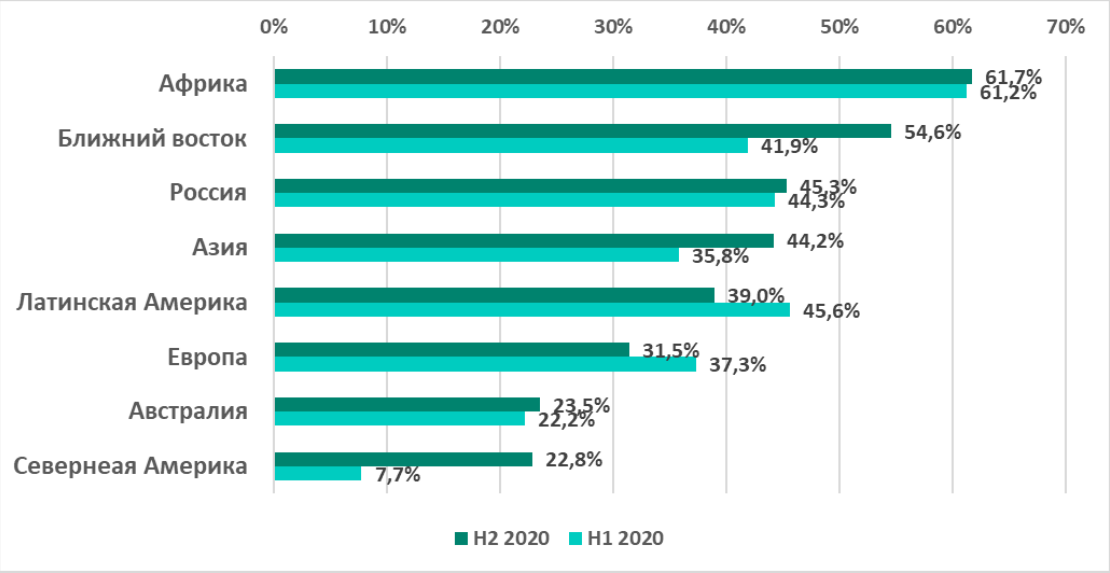


Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых индустриях, H2 2019 — H2 2020

Ландшафт угроз для компьютеров, используемых для инжиниринга и интеграции АСУ ТП, в значительной степени зависит от среды, в которой они находятся, в том числе их географического расположения, возможности доступа к внешним сетям и службам, а также поведения пользователей.

География

Максимальный процент компьютеров инженеров и интеграторов АСУ ТП, на которых было заблокировано вредоносное ПО, во втором полугодии 2020 года был в Африке (61,7%) и на Ближнем Востоке (54,6%). Россия в рейтинге регионов по этому показателю заняла третье место с показателем 45,3%.



Рейтинг регионов по проценту компьютеров, на которых было заблокировано вредоносное ПО в секторе инжиниринга и интеграции АСУ ТП, второе полугодие 2020

В Латинской Америке, на Ближнем Востоке, в Азии и Северной Америке процент компьютеров инженеров и интеграторов АСУ ТП, на которых было заблокировано вредоносное ПО, во втором полугодии 2020 года вырос по сравнению с первым полугодием 2020 года.

Самый высокий рост этого показателя — на 15,1 п.п. с 7,7% до 22,8% — был отмечен в Северной Америке. В основном он был обусловлен увеличением количества заблокированных веб-майнеров.

На Ближнем Востоке процент компьютеров, на которых было заблокировано вредоносное ПО в секторе инжиниринга и интеграции АСУ ТП, за полугодие увеличился на 12,7 п.п. с 41,9% до 54,6%. Рост произошел в основном из-за червей Fast-Load AutoLISP, которые распространяются вместе с зараженными проектами AutoCAD, а также из-за других червей, самораспространяющихся через USB.

Компьютеры инженеров АСУ ТП в южной и восточной Европе в основном сталкивались с фишинговыми письмами, которые использовались для доставки шпионского ПО и криптомайнеров. В этом вредоносном ПО реализованы различные методы распространения по сети (как в ручном, так и в автоматическом режимах), в частности:

- кража учетных данных пользователей при помощи Mimikatz и использование полученных данных для авторизации на других компьютерах в сети;

- эксплуатация уязвимостей в сетевых сервисах (SMB, MS SQL, RDP и т. д.);
- авторизация на других компьютерах в сети путем подбора пароля по словарю.

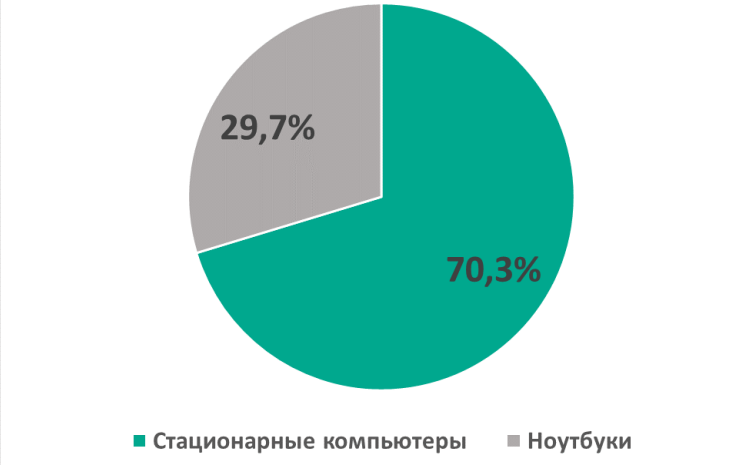
В Африке, России и в Европе процент компьютеров инженеров АСУ, на которых было заблокировано вредоносное ПО, во втором полугодии 2020 года был ниже, чем в первом полугодии.

Окружение

Окружение (среда), в которой находится компьютер инженера АСУ ТП, существенно влияет на ландшафт угроз. Например, очевидно, что изолированный компьютер менее уязвим для атак, чем компьютер, имеющий доступ к интернету или используемый за пределами защищенного периметра сети (например, ноутбуки).

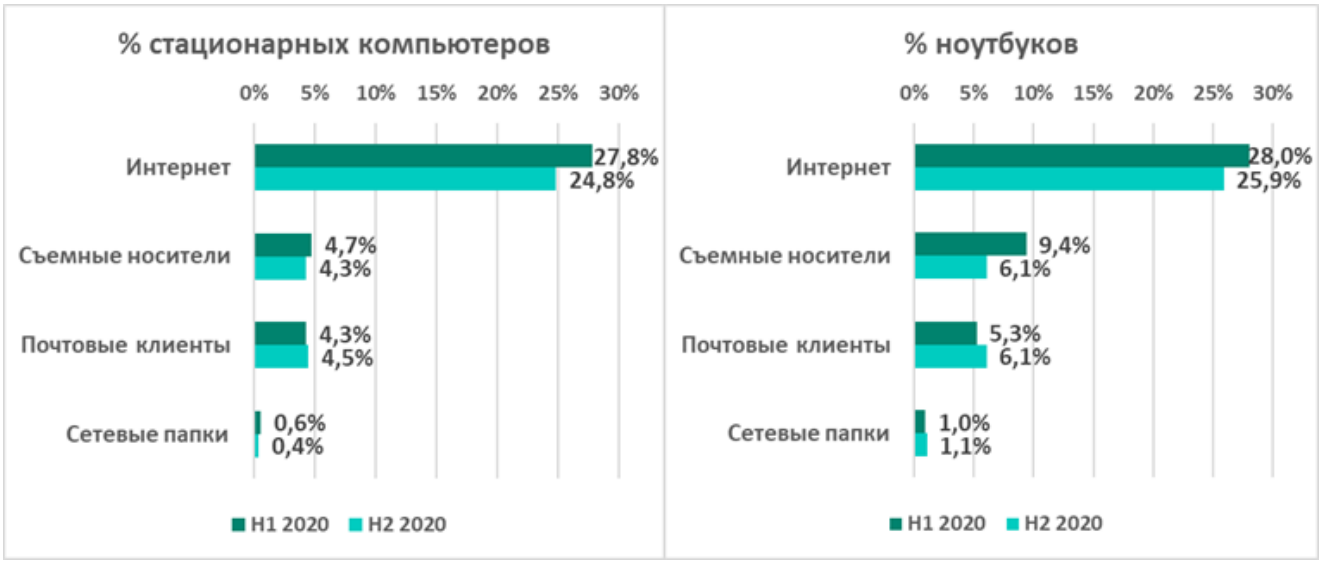
Ноутбуки и стационарные компьютеры инженеров АСУ

Анализ компьютеров инженеров АСУ из нашей выборки показал, что доля ноутбуков в этой выборке составляет 29,7%, а доля стационарных компьютеров соответственно 70,3%.



Соотношение стационарных компьютеров и ноутбуков среди компьютеров инженеров АСУ, H2 2020

На ноутбуках инженеров АСУ мы видим более высокий, чем на стационарных компьютерах, уровень угроз, связанных с интернет-контентом, съемными носителями, почтовыми клиентами и сетевыми папками.

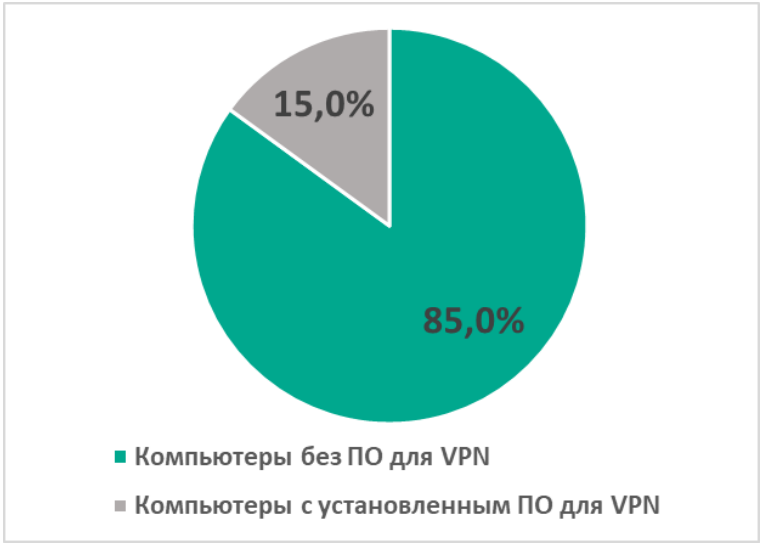


Процент компьютеров инженеров АСУ, на которых было заблокировано вредоносное ПО из разных источников. Стационарные компьютеры vs. ноутбуки, H1-H2 2020

Такое положение дел во многом связано с тем, что ноутбуки инженеров менее защищены (более уязвимы для атак), чем стационарные компьютеры. В то же время ноутбуки обычно имеют те же права и доступ, что и более защищенные стационарные компьютеры инженеров АСУ ТП.

Использование ПО для VPN

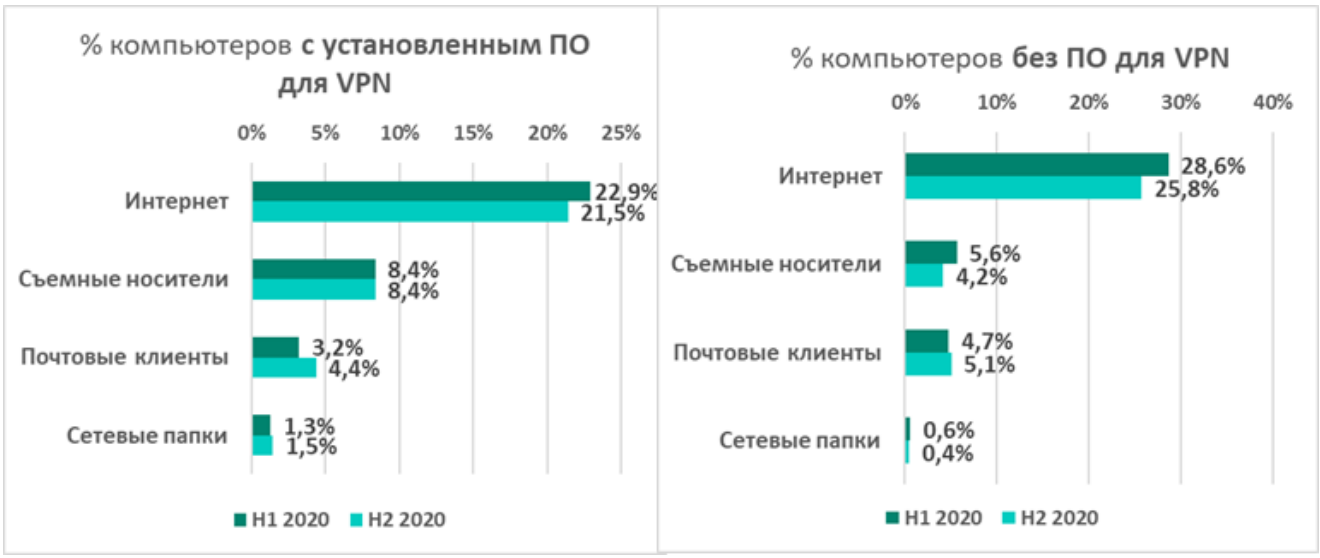
Ноутбуки и стационарные компьютеры инженеров АСУ можно разделить на две группы — те, которые используют ПО для VPN (15%), и те, которые не используют ПО для VPN (85%).



Соотношение компьютеров инженеров АСУ, использующих и не использующих ПО для VPN, H2 2020

Компьютеры инженеров, использующие ПО для VPN, явно имеют меньшую поверхность атаки — в частности, эти компьютеры в меньшей степени сталкиваются с интернет-угрозами (зараженными веб-сайтами, вредоносной рекламой и пр.) по сравнению с компьютерами, которые не используют ПО для VPN. Вероятно, это связано с тем, что те, кто использует программное обеспечение VPN, как правило, больше заботятся о безопасности. Также возможно, что конфигурация их VPN-туннеля перенаправляет весь трафик через туннель, в результате часть интернет-угроз может быть отфильтрована.

В то же время на компьютерах инженеров, использующих ПО для VPN, процент угроз, заблокированных на съемных носителях и в сетевых папках, выше, чем на компьютерах инженеров, которые не используют ПО для VPN.

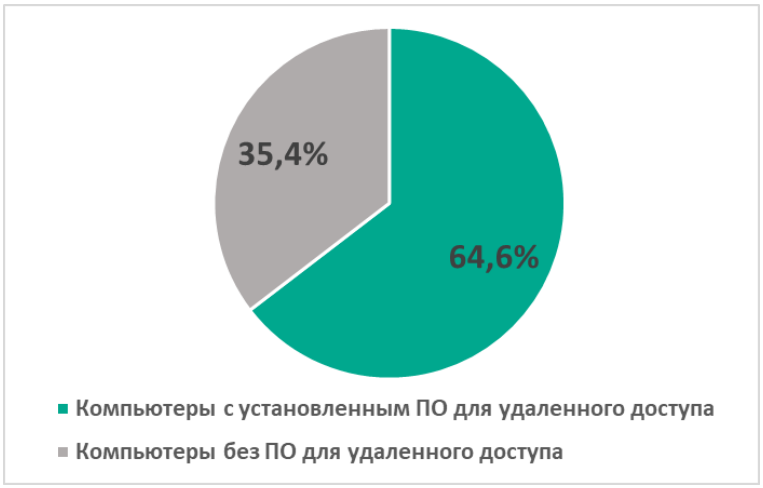


Процент компьютеров инженеров АСУ, на которых было заблокировано вредоносное ПО из разных источников. Компьютеры с ПО для VPN vs. компьютеры без ПО для VPN, H1-H2 2020

Различные вирусы и черви, существующие в среде АСУ в течение длительного времени и распространяющиеся через USB-устройства или сетевые папки, время от времени поражают компьютеры инженеров АСУ. Согласно имеющейся у нас статистике такие угрозы чаще блокировались на компьютерах инженеров, использующих ПО для VPN.

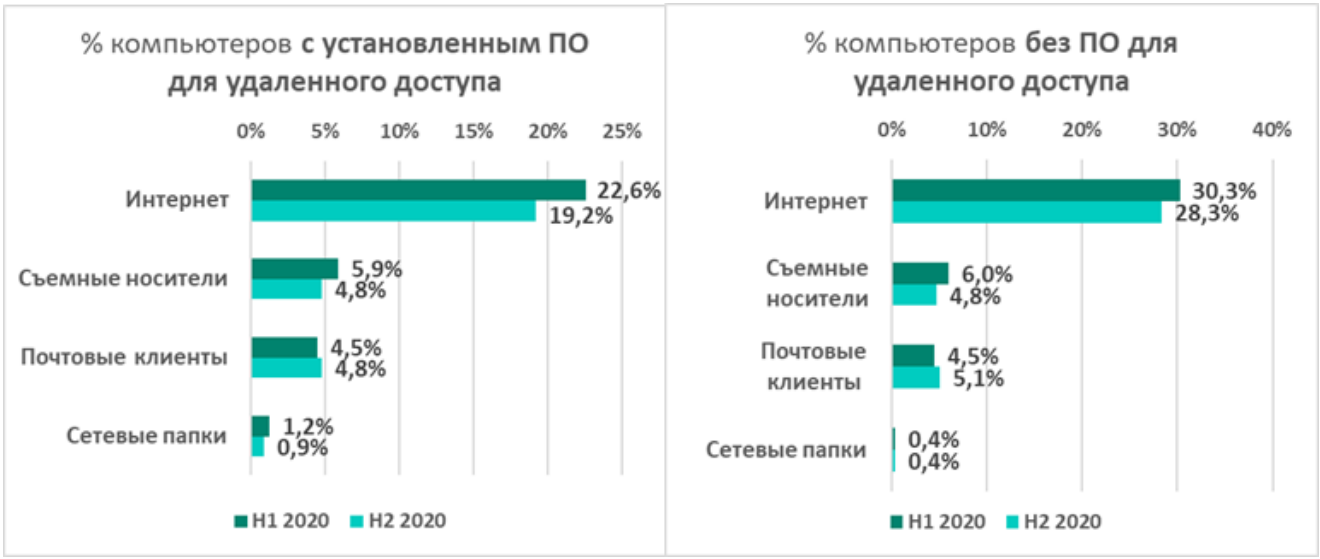
Использование ПО для удалённого доступа

Мы провели такой же анализ двух групп компьютеров инженеров АСУ — с программным обеспечением удаленного доступа и без него (64,6% и 35,4% соответственно).



Соотношение компьютеров инженеров АСУ, использующих и не использующих ПО для удаленного доступа, H2 2020

Обе группы (компьютеры инженеров, использующих и не использующих ПО для удаленного доступа) имеют довольно схожий ландшафт угроз, за исключением интернет-угроз (обычно доставляемых вместе с интернет-контентом).



Процент компьютеров инженеров АСУ, на которых было заблокировано вредоносное ПО из разных источников. Компьютеры с ПО для удаленного доступа vs. компьютеры без ПО для удаленного доступа, H1-H2 2020

Среди компьютеров инженеров, использующих ПО для удаленного доступа, процент компьютеров, на которых были заблокированы угрозы из интернета, значительно ниже, чем на компьютерах, не использующих ПО для удаленного подключения.

При этом детальный анализ угроз показал, что для компьютеров, использующих ПО для удаленного подключения, в большей степени характерны атаки на сетевые службы, такие как SMB, MS SQL и RDP. Большинство этих атак происходит из-за распространения червей в подсети (физической или виртуальной). Эти черви используют Mimikatz и распространяются по сети, переиспользуя украденные учетные данные, а также применяя эксплойты для уязвимостей в сетевых службах и проводя атаки подбора учетных данных.

Отметим, что некоторые компьютеры используют и ПО для удаленного подключения, и ПО для VPN. При этом такие компьютеры реже подключаются к интернет-ресурсам, чем компьютеры, которые не используют ПО для удаленного доступа.

Полный текст отчета доступен на портале **Kaspersky Threat Intelligence**
Чтобы получить больше информации, напишите нам на адрес **ics-cert@kaspersky.com**

Рекомендации

Чтобы обеспечить адекватную защиту систем АСУ, необходимо принять следующие меры:

- Убедитесь, что компьютеры инженеров и интеграторов АСУ ТП, особенно ноутбуки, хорошо защищены от сетевых атак, веб-угроз и фишинговых кампаний, включая целевые атаки. Для этого следует рассмотреть возможность внедрения современных технологий обнаружения угроз — как на уровне сетевого периметра, так и на всех сетевых узлах внутри периметра и всех удалённых сетевых узлах, имеющих доступ к локальной сети предприятия.
- Своевременно устанавливайте все обновления операционной системы и прикладного ПО, уделяйте особое внимание установке обновлений безопасности или применяйте обходные меры защиты там, где установка обновлений невозможна.
- Регулярно обучайте сотрудников тому, как выявлять подозрительные почтовые сообщения и вложения, подозрительную активность на компьютере, а также тому, как сообщать об инцидентах ответственным за информационную безопасность.
- По возможности ограничьте использование не производственного ПО, которое может представлять угрозу и/или содержать уязвимости, т.е. расширяет поверхность атаки. В частности, крайне

желательно ограничить использование ПО для удаленного доступа, офисное ПО, а также системное ПО, часто используемое в атаках, — PowerShell, Windows Script Host и т.д.

- Осуществляйте мониторинг выполнения файлов в организации и применяйте контроль программ в режиме Default Deny.
- Ограничьте использование USB-устройств, применяя метод белого списка, т.е. разрешая подключение только определённых безопасных устройств. Следует контролировать выполнение таких ограничений. Многие современные инструменты защиты конечных точек предоставляют возможность контроля подключаемых устройств.
- Используйте разные учетные записи для разных пользователей. Управляйте правами пользователей и служебных учетных записей таким образом, чтобы предотвратить распространение заражения по сети предприятия в случае взлома одной из учетных записей. Ведите журналы и проводите мониторинг использования прав локального и доменного администратора.
- Ограничьте права пользователей на их системах и права доступа к корпоративным сервисам с сохранением у каждого сотрудника минимального набора прав, необходимого ему для выполнения служебных обязанностей.
- Максимально возможно дифференцируйте права доступа. Ограничьте использование учетных записей с привилегированным уровнем прав. Администраторам следует по возможности использовать учетные записи с локальными правами администрирования или с правами на администрирование конкретных сервисов, избегая использования учетных записей с правами администратора домена.
- Осуществляйте аудит использования учетных записей с привилегированным уровнем прав и регулярно пересматривайте права доступа.
- Применяйте групповые политики, требующие регулярного изменения паролей пользователями. Введите требования к сложности паролей.
- Установите настройки операционной системы, при которых всегда показываются расширения файлов всех типов.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com