



# APT-атаки

# на промышленные компании в России

## Обзор тактик и техник

## 2019

[ptsecurity.com](http://ptsecurity.com)

## Содержание

Об исследовании	2
Промышленность под угрозой	4
Как начинается атака	6
На связи с командным центром	8
Успех необходимо закрепить	9
Высокие привилегии — большие возможности	9
Как найти администратора домена	10
Маскировка и еще раз маскировка	11
Как шпионы крадут данные	11
Самое слабое звено	11
Саботаж и его последствия	13
План Б	13
Как не стать жертвой АРТ	14
Тепловая карта тактик и техник АРТ-атак (группировки, атакующие промышленные компании)	15
Тепловая карта тактик и техник АРТ-атак (все группировки, атакующие компании в России)	16



## Об исследовании

Ранее мы уже рассказывали о том, что такое сложные целенаправленные атаки (атаки типа advanced persistent threat, АРТ-атаки), какие инструменты используют злоумышленники для таких атак, и оценили, сколько они могут стоить. Мы пошли дальше и проанализировали поведение 22 АРТ-группировок, атаковавших российские организации на протяжении последних двух лет<sup>1</sup>.

Среди целей этих группировок множество организаций, входящих в списки крупнейших компаний России и являющихся лидерами в своих отраслях. В предыдущей части мы подробно рассмотрели техники атак на финансовый сектор. В фокусе данного исследования промышленные компании, они находятся под прицелом у 13 АРТ-групп. Некоторые группировки проводили атаки на компании в России несколько лет назад, а в настоящее время переключили свое внимание на другие регионы. Они до сих пор активны, и мы включили их выборку, поскольку они вполне могут возобновить атаки на российскую промышленность.



68%

Государственные учреждения



59%

Промышленные компании



45%

Финансовая отрасль



41%

Топливо-энергетический комплекс

Распространенные категории жертв (доля атакующих АРТ-группировок)

Каждую АРТ-группировку можно охарактеризовать уникальной совокупностью мотивов, инструментов и методов, однако у всех киберпреступников есть и общие черты. В этом отчете рассмотрена специфика АРТ-атак на промышленную отрасль: на производственные и обрабатывающие предприятия, заводы и прочие индустриальные объекты. Мы хотим показать — как будет, скорее всего, действовать атакующая группа, если решит взломать вашу организацию. И конечно, предложим вариант защиты.

**АРТ-атака на промышленность** — это сложная целенаправленная атака на технологические или информационные системы промышленного предприятия, как правило для получения контроля над ними и нарушения их работоспособности либо с целью проведения конкурентной разведки. Кроме того, промышленная компания может быть атакована финансово мотивированной группой.

1. Опыт экспертов Positive Technologies показывает, что интервал до двух лет позволяет составить наиболее актуальную картину тактик и техник атаки.

Поведение АPT-группировок описано в соответствии с [MITRE ATT&CK \(Enterprise\)](#). Злоумышленники выбирают техники в зависимости от собранных на этапе разведки сведений об атакуемой организации, своего опыта и инструментов. В случае неудачи в ход идут альтернативные техники.

**MITRE ATT&CK** — это база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных АPT-атак. Представляет собой наглядную таблицу тактик, для каждой из которых указан список возможных техник. Позволяет структурировать знания об АPT и категоризировать действия злоумышленников.

В конце отчета мы привели тепловые карты (heat maps), основанные на матрице MITRE ATT&CK. Они дают представление о техниках, наиболее часто используемых в АPT-атаках на промышленные предприятия и на российские компании в целом.

Данные для анализа получены в ходе расследований киберинцидентов и работ по ретроспективному анализу событий безопасности в инфраструктуре различных компаний, а также в ходе постоянного отслеживания активности действующих сегодня АPT-группировок экспертами Positive Technologies Expert Security Center. Дополнительно использовалась информация из общедоступных отчетов о деятельности АPT-группировок, подготовленных ведущими компаниями в области ИБ.

Кроме того, мы провели опрос<sup>2</sup> среди посетителей сайта компании Positive Technologies, аудитории интернет-портала [SecurityLab.ru](#)<sup>3</sup> и участников ряда отраслевых сообществ, в которые входят эксперты по ИТ и ИБ из различных сфер отечественного бизнеса, — чтобы оценить готовность российских компаний к противостоянию сложным целенаправленным атакам. Ответы респондентов из промышленных и топливно-энергетических компаний представлены далее.

2. В опросе приняли участие 306 респондентов. Доля представителей промышленности и топливно-энергетического комплекса составила 18,6%.

3. Сайт SecurityLab.ru — один из лидеров российского интернета в сфере информационной безопасности. Ежемесячная аудитория портала насчитывает около полумиллиона посетителей, большая часть из которых — программисты, специалисты по ИТ и ИБ, руководители соответствующих отделов.



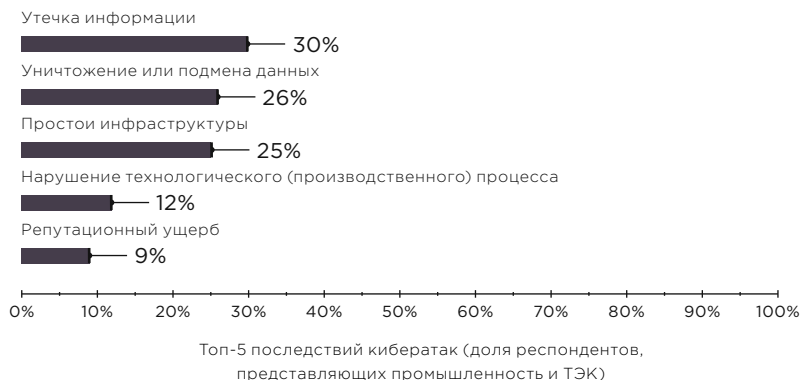
## Промышленность под угрозой

Промышленность сегодня динамично развивается. По данным Росстата, в первом полугодии 2019 года индекс промышленного производства в России вырос на 2,6 процентного пункта. В 2019 году на обеспечение государственной программы «Развитие промышленности и повышение ее конкурентоспособности» выделено 313,3 млрд рублей, из них 204,8 млрд — на развитие автомобилестроения. Очевидно, что индустриальный сектор составляет основу экономики, и его благополучие имеет важное значение для стабильности государства. Угроза нарушения работы промышленных предприятий ставит под удар как экономику государства, так и его репутацию, и промышленные компании могут стать жертвами целенаправленных кибератак.

### По каким причинам ваша компания может стать целью АРТ-группировок?

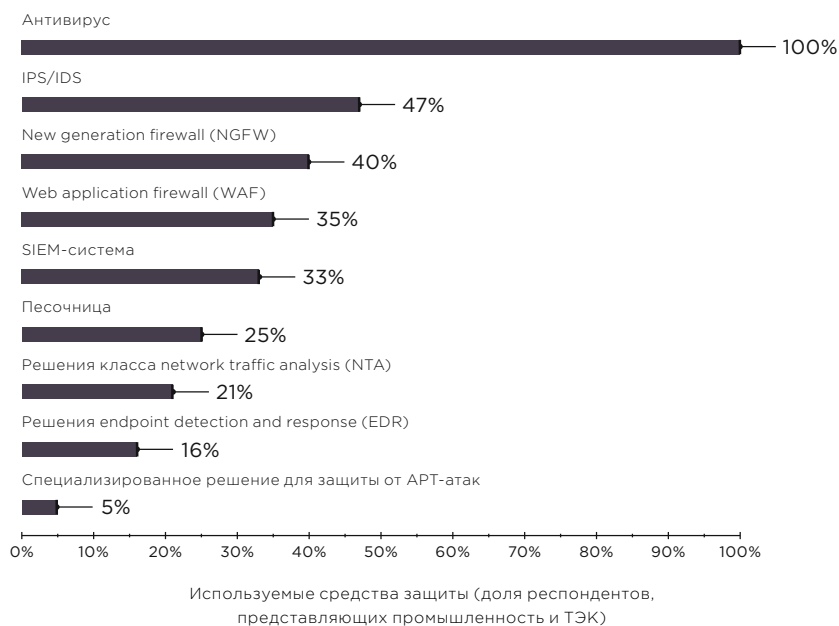


### С какими последствиями кибератак сталкивалась компания?



АРТ-атаки проводят кибергруппировки, в которых каждый участник имеет свою специализацию, но всех их объединяет богатый опыт взлома компьютерных систем. При этом в некоторых промышленных компаниях до сих пор используются лишь базовые средства защиты, которые малоэффективны в борьбе против сложных угроз.

### Какие технические средства защиты информации применяются в компании?



Успех APT-атаки зависит, в числе прочего, от уровня осведомленности сотрудников компании в вопросах кибербезопасности. Каждый третий участник нашего опроса (32%), представляющий промышленный и топливно-энергетический комплексы, отметил, что в компании не проводится обучение по вопросам кибербезопасности, а 44% респондентов констатировали, что такое обучение проводится лишь формально, его качество не проверяется.

Чтобы эффективно бороться с высококвалифицированными злоумышленниками, важно понимать, как они действуют. Необходим оперативный обмен информацией о киберинцидентах между компаниями внутри отрасли. Однако большинство организаций промышленной сферы сегодня не готовы делиться такими сведениями. Например, в 73% промышленных компаний в российских регионах информация о киберинцидентах не раскрывается.

Уровень квалификации специалистов в области ИБ, работающих в компании, имеет немаловажное значение для защиты от целенаправленных атак. Однако 46% участников нашего опроса, представляющих промышленность и топливно-энергетический комплекс, признали, что квалификация специалистов по ИБ в компании недостаточна для выявления и расследования киберинцидентов. Кроме того, 23% участников опроса отметили, что в их компаниях практика выявления и расследования инцидентов ИБ и вовсе отсутствует.

Более половины (60%) респондентов из сферы промышленности и топливно-энергетического комплекса признают, что риск успешной кибератаки является критически значимым. Каждый четвертый (23%) респондент считает, что защита от APT-атак является приоритетным направлением развития ИБ в организации. Однако только 11% участников опроса выразили уверенность в том, что предприятие сможет противостоять APT-группировкам.

Если ваша компания стала целью APT-группы, то высокая мотивация и серьезный уровень подготовки злоумышленников рано или поздно дадут результат, и им удастся проникнуть в вашу инфраструктуру. Но



если взлом неизбежен, то важно уметь вовремя распознать начавшуюся атаку и преградить злоумышленникам дорогу к критически важным системам и данным.

## Как начинается атака

Чтобы попасть во внутреннюю сеть, взломщикам необходима «точка входа» — компьютер, который они заразят вредоносным ПО и с которого начнут дальнейшее перемещение по сети организации. Большинство группировок (85%) пытаются доставить вредоносное ПО с помощью фишинга, то есть путем рассылки электронных писем, цель которых — вынудить получателя открыть приложенный файл (spearphishing attachment) или перейти по ссылке (spearphishing link).

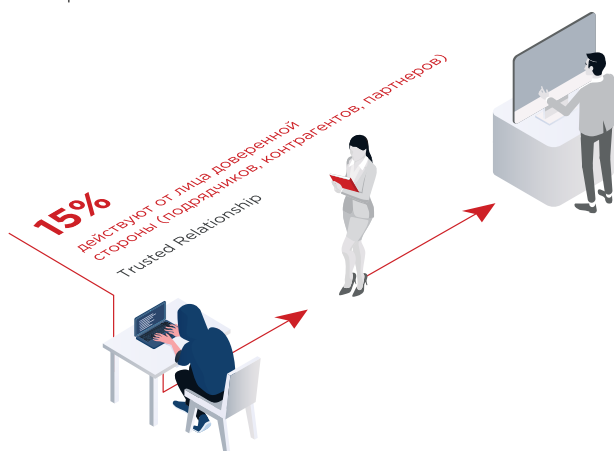


Злоумышленники тщательно готовятся к фишинговой атаке. Группировка SongXY, например, рассылала документ, открыв который сотрудник невольно сообщал злоумышленникам IP-адрес своего компьютера и версию установленного на нем Microsoft Office. Таким образом злоумышленники собирали информацию, которая помогала им подобрать подходящий инструмент для последующих этапов атаки.

Существуют и другие методы проникновения во внутреннюю сеть. Например, 31% АРТ-групп, атакующих промышленные компании, используют технику drive-by compromise. В ходе такой атаки на компьютер сотрудника во время просмотра зараженного сайта незаметно загружается вредоносное ПО. Чтобы повысить вероятность успеха, злоумышленники постараются заразить вредоносным ПО именно те сайты, которые часто посещают сотрудники компании-жертвы. Эта разновидность атак типа drive-by называется watering hole, или strategic web compromise.



Автоматизация процессов внутри предприятий сопряжена с внедрением специализированного оборудования и программного обеспечения, для которого требуется квалифицированная техническая поддержка. Промышленные компании вынуждены обращаться за ней к подрядчикам. Но далеко не все осознают угрозу, которая за этим стоит. Ведь скомпрометировав подрядчика, имеющего удаленный доступ к внутренней сети вашей компании, злоумышленник автоматически получает «пропуск», который позволит ему выполнять действия от имени взломанного поставщика услуг. Техника называется *trusted relationship*, ее используют 15% АPT-групп. Другой пример ее возможной реализации — взлом компании-партнера и рассылка фишинговых писем от его имени; это повышает шансы на то, что вредоносное послание откроют.



Некоторые группы (15%) доставляют вредоносное ПО в инфраструктуру вместе с поставками оборудования или обновлениями программного обеспечения (техника *supply chain compromise*). Например, в первом полугодии 2019 года стало известно, что киберпреступники добавили вредонос в утилиту ASUS Live Update, с помощью которой загружаются обновления на компьютеры ASUS. Инцидент оставался незамеченным в течение пяти месяцев, за это время заражены оказались более полумиллиона компьютеров по всему миру.



Стоит отметить, что компания и сама может стать начальным звеном в цепочке атак, если цель группировки — ее заказчик или партнер. Например, известно, что масштабная кампания Stuxnet началась со взлома пяти промышленных компаний, поставляющих оборудование для топливно-энергетического комплекса.



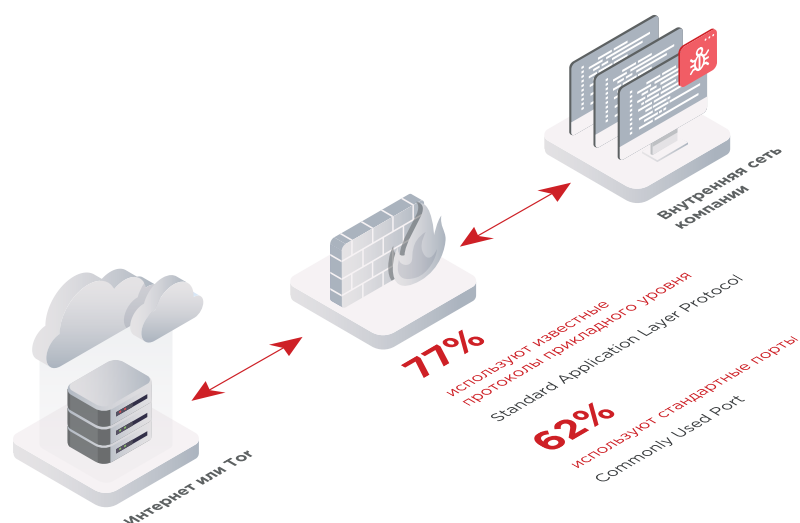
## На связи с командным центром

После проникновения в инфраструктуру задача номер один для злоумышленников — наладить канал связи с командным центром (C&C, C2-сервером).

### Г Что такое командный центр (C&C, C2)

Это один или несколько серверов, с которых злоумышленники управляют атакой. С помощью C2-сервера взломщики отправляют директивы в зараженные системы, устанавливают, обновляют и удаляют вредоносное ПО. На эти серверы отправляется вся похищенная злоумышленниками информация.

Командный центр злоумышленников может находиться в интернете либо в анонимной сети Tor. Взломщики стараются избежать блокировки трафика, которым обмениваются C2-серверы и скомпрометированные компьютеры, со стороны межсетевого экрана. В этом им помогает маскировка вредоносного трафика под легитимный. Три четверти АРТ-группировок (77%) обмениваются информацией с C2-сервером по известным протоколам прикладного уровня (standard application layer protocol). Большая часть (62%) группировок используют стандартные порты (commonly used port). Например, загрузчик CMstar группировки SongXY доставляется на компьютер жертвы по протоколу HTTP.



Большинство APT-группировок шифруют канал связи с C2-серверами, чтобы скрывать вредоносный трафик. Каждая вторая группа (46%) с этой целью использует известные алгоритмы (standard cryptographic protocol), например RC4 или простое XOR-суммирование, а 38% — их модифицированные версии (custom cryptographic protocol).

## Успех необходимо закрепить

После проникновения во внутреннюю сеть злоумышленникам необходимо предпринять меры для того, чтобы надолго остаться в инфраструктуре, даже если компьютеры будут перезагружены, а пароли сотрудников изменены. Почти все APT-группировки (89%) обеспечивают автозапуск своего вредоносного ПО после перезагрузки зараженного компьютера, добавляя ключи реестра (registry run keys / startup folder). Опуская технические детали, отметим, что, например, троян RTM использует эту технику по-разному в зависимости от уровня привилегий пользователя на компьютере жертвы. Однако независимо от привилегий, с которыми запускается троян, техника registry run keys комбинируется с другой техникой — rundll32, которую используют 46% APT-групп, включая упомянутую группировку RTM.



### Как работает связка техник registry run keys и rundll32

Для выполнения функций из динамически подключаемых библиотек (DLL) в Windows предусмотрен системный компонент rundll32.exe. Он может использоваться злоумышленниками как инструмент для автозапуска вредоносных программ из DLL-файлов путем добавления соответствующих ключей в подразделы Run и RunOnce реестра Windows.

Группировка TaskMasters для закрепления в инфраструктуре создает резервные каналы связи с командным центром (техника redundant access).

## Высокие привилегии — большие возможности

Действия злоумышленников требуют выполнения команд и запуска различного ПО, а значит — привилегий обычного пользователя киберпреступникам будет недостаточно. Злоумышленники придумали способы выполнять необходимые им действия с правами администратора. Каждая вторая группировка (46%) с этой целью внедряет вредоносные скрипты и команды в контекст процессов, запущенных с правами администратора (process injection), а каждая четвертая (23%) ищет способы обойти защитный компонент UAC в Windows, ответственный за контроль учетных записей (bypass user account control). Например, загрузчик группировки APT37 снабжен инструментом UACME, который



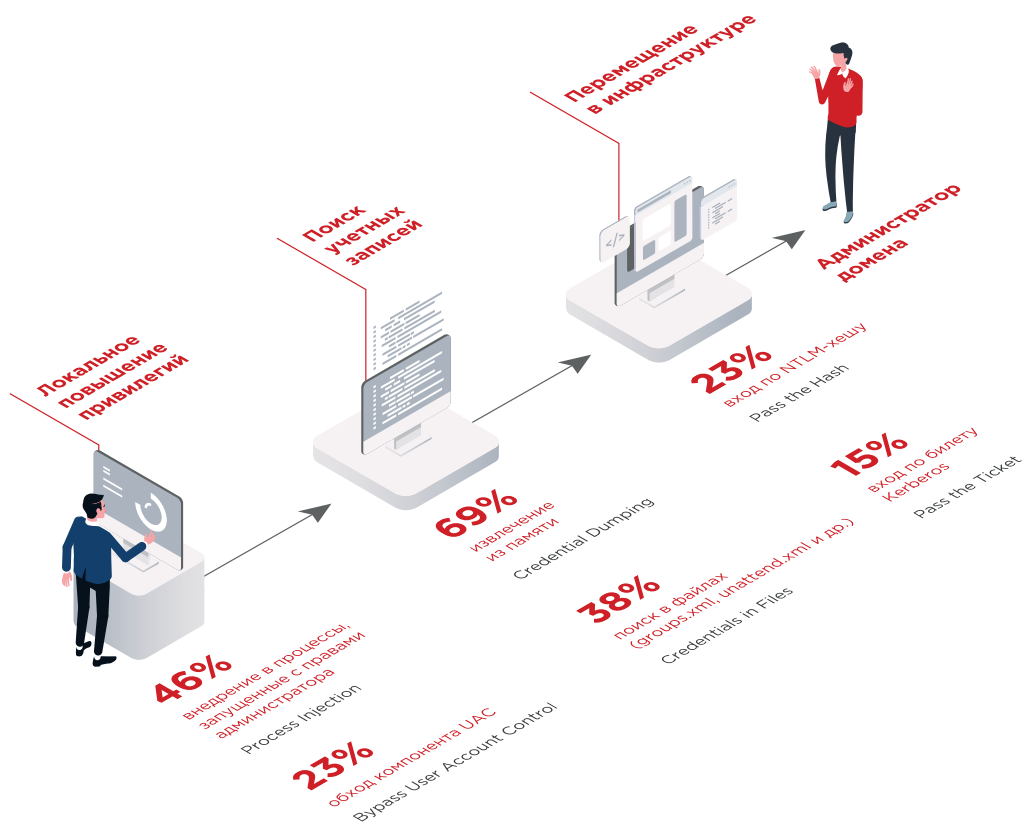
позволяет запустить полезную нагрузку вредоноса в привилегированном режиме.

После закрепления в системе и повышения локальных привилегий злоумышленники пойдут дальше — постараются найти компьютеры ключевых лиц компании и серверы, на которых хранится ценная информация. Кроме того, киберпреступники будут искать «точки входа» в сегмент сети, где расположены системы управления технологическими процессами.

## Как найти администратора домена

Компьютеры в корпоративной сети, как правило, объединены в домены. Администратор домена имеет максимальные привилегии и доступ к информации на любом компьютере в нем. На компьютере, с которого был получен доступ во внутреннюю сеть, злоумышленники будут искать учетные данные, чтобы попасть в другие системы, а попав в них — постараются найти там новую порцию учетных данных. Так будет продолжаться до тех пор, пока злоумышленники не найдут учетную запись администратора домена.

Как злоумышленники ищут учетные данные? Они могут получать их из разных источников. Так, группировка TaskMasters использует утилиту GsecDump для извлечения хешей паролей к учетным записям из базы данных Security Account Manager и Active Directory. Технику извлечения паролей, как правило в виде хеш-значений, из оперативной памяти или памяти запущенных процессов (credential dumping) используют 69% APT-группировок. Восстанавливать пароли по их хеш-значениям злоумышленникам не потребуется: существуют техники входа по NTLM-хешу или билету Kerberos; их используют как минимум 23% и 15% группировок соответственно.



## Маскировка и еще раз маскировка

Поиск учетной записи администратора домена, а также узлов, с которых есть доступ к промышленным системам, предполагает активное перемещение по сети. Но одно неосторожное действие приведет к обнаружению средствами защиты, поэтому каждая вторая APT-группировка (54%) старается их отключить, переконфигурировать или как-то иначе нарушить их работоспособность. Например, троян группировки RTM проверяет на скомпрометированном компьютере наличие антивируса ESET. Если антивирус установлен, троян повреждает его лицензионный файл и затем этот файл удаляет.

Для выполнения действий в системе злоумышленники по возможности будут обходиться без установки программ на компьютер жертвы, так как их сложно скрыть от средств защиты. Там, где можно обойтись без файлов, они используют так называемые бестелесные техники. Например, 54% APT-группировок запускают скрипты PowerShell, а 31% используют WMI. Эти инструменты популярны у злоумышленников, поскольку ими пользуются IT-специалисты, а следовательно, действия атакующих, когда они используют PowerShell и WMI, сложно отличить от легитимных действий.

Некоторые группировки (15%) используют технику data obfuscation, направленную на затруднение анализа вредоносного трафика. Например, группировка APT37 применяет для защиты C&C-коммуникаций методы стеганографии: загрузчик скачивает на компьютер жертвы изображение, в котором зашифрована полезная нагрузка.



**62%**

устанавливают кейлоггеры  
Input Capture

**62%**

делают скриншоты  
Screen Capture

**31%**

контролируют микрофон  
Audio Capture

**8%**

записывают видео  
Video Capture

## Как шпионы крадут данные

Добравшись до узлов, которые могут стать источником ценной информации (схем, чертежей и расчетов, паролей для доступа к критически важным системам, сведений об объемах производства и финансовой отчетности), злоумышленники установят шпионское ПО. Например, зловред Gh0st группировки SongXY обладает стандартным набором функций шпионского трояна: делает скриншоты, записывает звук с микрофона и видео с веб-камеры. Под угрозой компьютеры руководства, бухгалтерии, инженеров и администраторов, у которых есть доступ к промышленным системам.

Некоторые трояны выполняют также функцию кейлоггеров — перехватывают нажатия клавиш пользователей и отправляют их на серверы злоумышленников. С помощью кейлоггеров киберпреступники могут контролировать переписку, которая ведется с зараженного компьютера, перехватывать введенные логины, пароли и другую чувствительную информацию. Так, кейлоггер группировки RTM умеет отслеживать нажатия клавиш не только физической клавиатуры, но и виртуальной, а также способен перехватывать данные из буфера обмена.

## Самое слабое звено

Внутренняя сеть промышленной компании может состоять из тысяч устройств, но злоумышленников интересуют только те, на которых хранятся критически важные данные, и те, которые позволяют получить доступ к технологическим сегментам, чтобы управлять



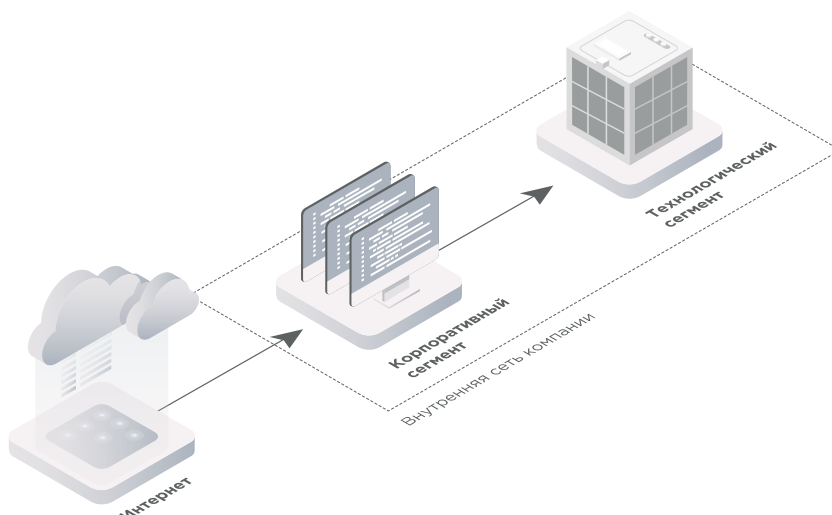
промышленными системами. Большинство группировок (69%) стремятся изучить топологию сети (system network configuration discovery) как можно раньше, чтобы не тратить время на взлом не интересующих их систем и снизить риск обнаружения.

Во внутренней сети промышленного предприятия можно выделить два основных сегмента — корпоративный и технологический. В корпоративном сегменте находятся компьютеры большинства сотрудников и серверы бизнес-приложений. Он интересует тех злоумышленников, которые пришли за новыми разработками в области промышленных технологий, и финансово мотивированные группировки.

Но атакующие постараются пойти дальше и будут искать способы проникнуть в технологический сегмент. Здесь находятся компьютеры операторов АСУ ТП, SCADA, контроллеры, инженерные станции и другие промышленные системы. Ни одно устройство в этом сегменте не должно быть доступно ни из интернета, ни из корпоративной сети. Однако так бывает далеко не всегда. На практике отдельные здания промышленного предприятия могут быть территориально разнесены на километры друг от друга, более того — они могут находиться в разных городах, поэтому IT-специалисты организуют себе удаленный доступ к устройствам технологического сегмента. Согласно [нашему исследованию](#), в 64% случаев недостатки сегментации сетей или фильтрации трафика были внесены администраторами при создании каналов удаленного управления.

Нередко для доступа к промышленным системам используются стандартные пароли — так называемые пароли по умолчанию. Пароли по умолчанию используются в 73% промышленных компаний. В этом случае даже установка кейлоггера не требуется: пароль подбирается методом перебора (brute force). Эту технику используют как минимум 15% группировок. Кроме того, при недостаточной осведомленности в вопросах ИБ сотрудники могут хранить пароли для доступа к промышленным системам прямо в текстовых файлах на своих компьютерах или сохранять параметры удаленного подключения, чтобы не вводить пароль снова.

Если в вашей компании наблюдается похожая ситуация, то безопасность под серьезной угрозой, ведь скомпрометировав компьютер сотрудника, имеющего доступ к технологическому сегменту, злоумышленники смогут управлять промышленными системами.



## Саботаж и его последствия

Попав в технологический сегмент, злоумышленники постараются повысить свои права на скомпрометированных компьютерах, закрепиться и затаиться с помощью техник, описанных выше. Злоумышленники могут годами контролировать инфраструктуру, оставаясь в тени. Выбрав подходящий момент, киберпреступники перейдут к активным действиям. Если их цель — саботаж, то в ход пойдет ПО, способное нарушить работоспособность компьютеров и оборудования. Например, в арсенале группировки [APT37](#) есть модуль RUNHAPPY, который перезаписывает загрузочную запись MBR и не дает операционной системе загружаться.

Простой инфраструктуры является крайне нежелательным последствием APT-атаки для промышленной компании. Согласно [отчету IBM X-Force IRIS](#), среднее время восстановления после разрушительного воздействия вредоносного ПО уровня NotPetya, Stuxnet, Shamoon или Dark Seoul составляет 512 часов, а средний ущерб от деструктивного ПО составляет 239 млн долл. США.

Заметая следы, злоумышленники могут заразить всю инфраструктуру, включая технологический сегмент, трояном-шифровальщиком. Так, норвежский металлургический завод [Norsk Hydro](#) столкнулся с шифровальщиком LockerGoga, который остановил производство. Ущерб составил порядка 41 млн долл. США. От атак шифровальщика LockerGoga пострадали также американские предприятия химической промышленности [Hexion](#) и [Momentum](#).

## План Б

Технологический сегмент может быть полностью изолирован как от корпоративного сегмента, так и от интернета. Тогда, если конечная цель злоумышленников находится именно в промышленном сегменте сети, в ход идет тяжелая артиллерия. В компанию могут быть подброшены съемные носители (например, флешки) с вредоносным ПО, или их может подключить к USB-разъемам критически важных систем внедрившийся в компанию инсайдер (техника replication through removable media). Так, несколько лет назад группировка Equation использовала бэкдор, позволяющий получать данные с компьютеров в изолированной сети. Механизм бэкдора заключается в следующем. Киберпреступники распространяли посредством USB-накопителей компьютерный червь Fanny. Троян создает на флешке скрытый сектор, куда собирается информация о сети, в которой находится компьютер. Когда флешка подключается к компьютеру с выходом в интернет, собранные данные передаются на C2-сервер злоумышленников. Также предусмотрен механизм для передачи информации в обратном направлении: в скрытый сектор атакующие могут добавить команды, которые выполняются при подключении флеш-накопителя к компьютеру в изолированной сети. Троян Fanny содержал эксплойт для неизвестной в то время уязвимости и успешно запускался даже на компьютерах с отключенной функцией автозапуска.

Заражения с помощью съемных накопителей актуальны и сегодня. Как показывают результаты отчета компании [Honeywell](#), 16% всех вредоносов, распространяющихся через USB-устройства, разработаны

специально для атак на промышленные системы. Техника заражения через USB-устройства особенно эффективна в изолированной инфраструктуре. Речь идет не только о флешках, но обо всех устройствах класса human interface devices (HID), к которому относятся клавиатуры, мыши и другие устройства.

## Как не стать жертвой АРТ

Большинство АРТ-группировок, атакующих сегодня российские промышленные предприятия, используют сложные техники, и шансы поймать преступников в момент их проникновения в компанию минимальны. Проникнув в корпоративную сеть, они действуют максимально скрытно и осторожно, замечают следы. Важно понимать, что злоумышленники могут не производить никаких действий на протяжении месяцев или нескольких лет, ожидая команды от заказчика атаки, который может преследовать в том числе и политические цели. Нельзя закрывать глаза на тот факт, что даже сегодня в вашей инфраструктуре могут прятаться злоумышленники. И ведь в этом случае остановить преступников еще не поздно, так как они не перешли к активной стадии атаки и деструктивным воздействиям на производство.

Но как обнаружить того, кто так старается не выдать себя? Здесь нужен особый подход, поскольку типовых решений для защиты серверов и рабочих станций в реальном времени (например, антивирусов или EDR) будет явно недостаточно. Нужно уметь взглянуть на события в прошлом, сопоставить их, выявить аномалии. Такой ретроспективный подход действительно дает результат.

Как это работает? На момент атаки сигнатуры для ее выявления еще не существовало, но сегодня она может быть уже известна. Нужно лишь уметь ее применить. Если есть возможность периодически проверять ранее полученные почтовые вложения и другие файлы, периодически запускать их проверку в песочнице, отслеживать сетевые аномалии не только в реальном времени, но и в ретроспективе, то не обнаруженные еще вчера угрозы сегодня могут быть выявлены. Такой подход позволяет не просто обнаружить зловред в системе — он помогает отследить всю цепочку атаки, постепенно раскручивая клубок событий и анализируя артефакты.

Чтобы предотвратить атаку в технологической сети на финальном этапе вредоносной кампании, когда злоумышленник уже начал выводить из строя промышленное оборудование, также нужны специализированные средства защиты. Необходимо использовать программно-аппаратный комплекс, который обеспечивает непрерывный мониторинг защищенности сети АСУ ТП, помогает на ранней стадии выявлять кибератаки, неавторизованные действия персонала, в том числе злонамеренные. И конечно, чем безопаснее организована сегментация технологической сети, чем строже администраторы безопасности следят за разграничением доступа и уровнем привилегий пользователей, своевременным обновлением ПО, тем сложнее преступникам атаковать такую сеть.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshsta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshsta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

80-100%60-80%40-60%20-40%0-20%

Тепловая карта тактик и техник АРТ-атак (группировки, атакующие промышленные компании)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Stored Data Manipulation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Transmitted Data Manipulation
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Firmware Corruption
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Resource Hijacking
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Network Denial of Service
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Endpoint Denial of Service
	Mshst	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshst							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänger							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							



# Тепловая карта тактик и техник АРТ-атак

(все группировки, атакующие компании в России)

## О компании

[ptsecurity.com](http://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/PositiveTechnologies](https://facebook.com/PositiveTechnologies)  
[facebook.com/PHDays](https://facebook.com/PHDays)

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.