



Риски ИБ в промышленных компаниях

ptsecurity.com

Атаки на промышленность

Промышленность привлекает злоумышленников своими масштабами, значимостью выполняемых бизнес-процессов, влиянием на окружающий мир и жизнь граждан. Например, техногенная авария на ГЭС может оставить без электричества целую страну, как в [случае с Венесуэлой](#), когда свет во всей стране погас на целых пять дней. А простой на автомобильном заводе может привести к крупным убыткам, как в истории с заводом Honda, подвергшимся [атаке вируса-шифровальщика](#). К счастью, кибератаки на промышленные компании с такими серьезными последствиями являются единичными, ведь они требуют повышенного уровня квалификации злоумышленников. Задача экспертов по информационной безопасности — сделать так, чтобы аварии на производстве не стали регулярными. Для этого необходимо определить недопустимые для компании события и обеспечить такой уровень ИБ, который будет гарантировать, что эти события не произойдут в результате кибератаки.

В 2020 году промышленная сфера была у хакеров второй по популярности после государственной: [по нашим подсчетам](#), на нее было направлено 12% атак.

Основными киберугрозами для промышленных компаний сегодня являются шпионаж и финансовые потери. Так, в 2020 году мотивом большинства атак (84% случаев) было получение данных, а финансовая выгода интересовала 36% хакеров.

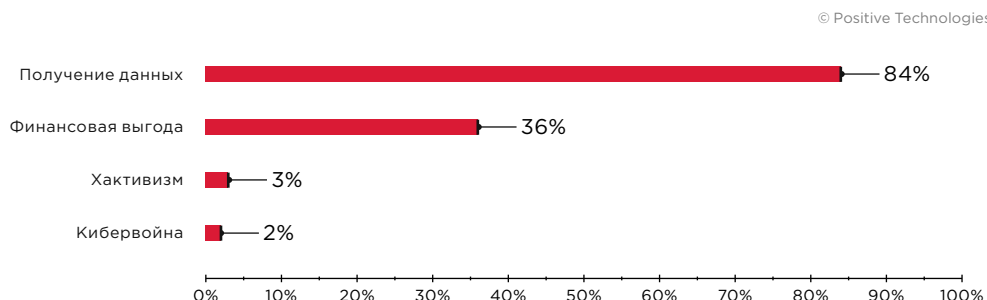


Рисунок 1. Мотивы кибератак на промышленные компании в 2020 году

Последствия кибератак могут быть существенны.

Остановка производства

Из-за обычного шифровальщика, запущенного в корпоративную сеть автопроизводителя Honda с целью получения выкупа, компании пришлось на целый день остановить производство на нескольких [заводах](#). После такого вмешательства у компании уйдет немало сил, чтобы вернуться к нормальной работе и обеспечить дальнейшее полноценное функционирование технологических и бизнес-систем, а также не допустить повторного вторжения.

Нарушение технологических процессов

В мае 2021 года в результате атаки вируса-шифровальщика была нарушена работа Colonial Pipeline — крупнейшего в США поставщика топлива. Из-за недельного простоя компьютерных систем компании закрылась половина заправочных станций в нескольких юго-восточных штатах, выросли оптовые цены на бензин, возник ажиотажный спрос на топливо. В 2020 году злоумышленники пытались атаковать системы водоснабжения и очистки воды в Израиле. А в феврале 2021 года одному хакеру удалось получить доступ к системам водоочистных сооружений в небольшом городе США и изменить химический состав воды.

Нарушение бизнес-процессов

В феврале 2020 года в результате хакерской атаки хорватская нефтяная компания INA не могла выставлять счета-фактуры, фиксировать использование карт лояльности, выпускать новые мобильные ваучеры и принимать от клиентов плату за топливо. Причиной нарушения бизнес-процессов стала программа-вымогатель Clor, зашифровавшая данные на внутренних серверах компании.

Главная задача, которая сегодня стоит перед специалистами по информационной безопасности, — оценить реализуемость различных недопустимых событий ИБ в компании и выявить возможные последствия кибератак, чтобы на основании этих знаний выстроить эффективную систему защиты. Вопрос в том, как это сделать, если любые действия в инфраструктуре, способные негативно повлиять на технологический процесс, никогда не будут согласованы руководством.

Оценка реализуемости рисков на киберполигоне

Киберучения — это контролируемые атаки, проводимые с целью проверки и улучшения навыков службы ИБ по обнаружению киберугроз и реагированию на них. Атаки на киберучениях The Standoff реализуются с привлечением десятков команд атакующих, состоящих из экспертов по информационной безопасности.

На киберполигоне The Standoff в мае 2021 года мы предложили командам атакующих реализовать риски ИБ на инфраструктуре газораспределительной станции. Условия были максимально приближены к реальным. Например, даже сетевое взаимодействие происходило по распространенным протоколам АСУ ТП (OPC DA, Modbus TCP, UMAS, IEC 60870-5-101, Siemens Simatic S7, Siemens DIGSI, Vnet/IP, CIP (EtherNet/IP), IEC 61850, BACnet/IP), по SNMP и, конечно, по HTTP.

Чтобы нарушить технологический процесс подачи газа, атакующим потребовалось два дня. Получив доступ к системе управления газовой станцией, хакеры остановили процесс подачи газа и устроили взрыв. Ежедневно в офисе компании защитники фиксировали в среднем 32 инцидента.

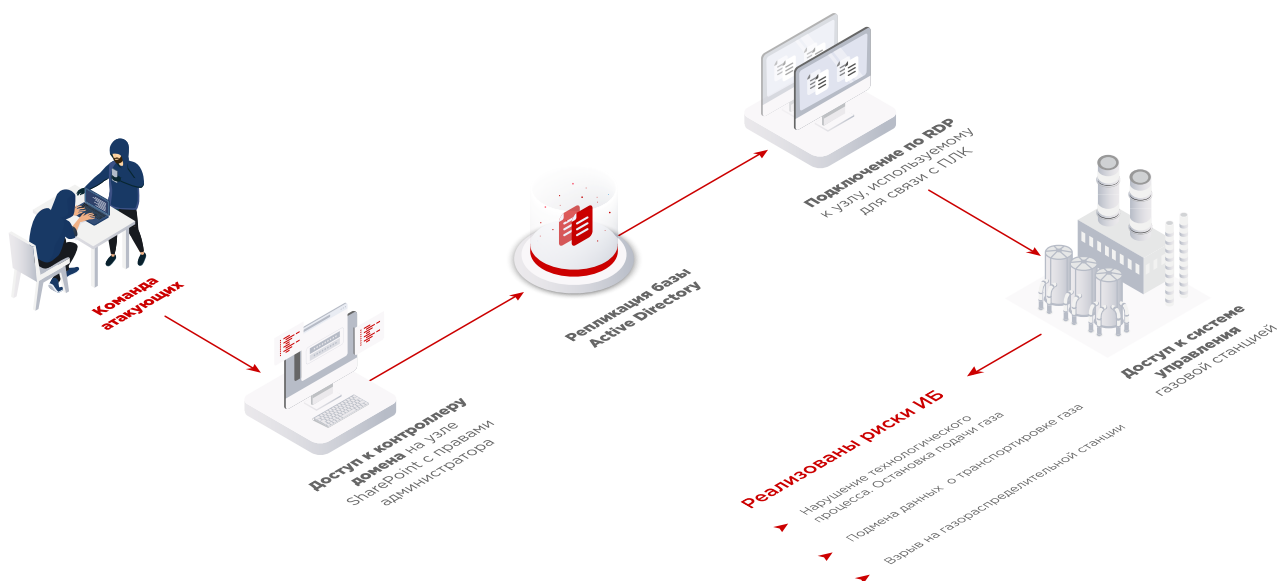


Рисунок 2. Упрощенная схема сценария реализации рисков ИБ для газораспределительной станции в рамках The Standoff 2021

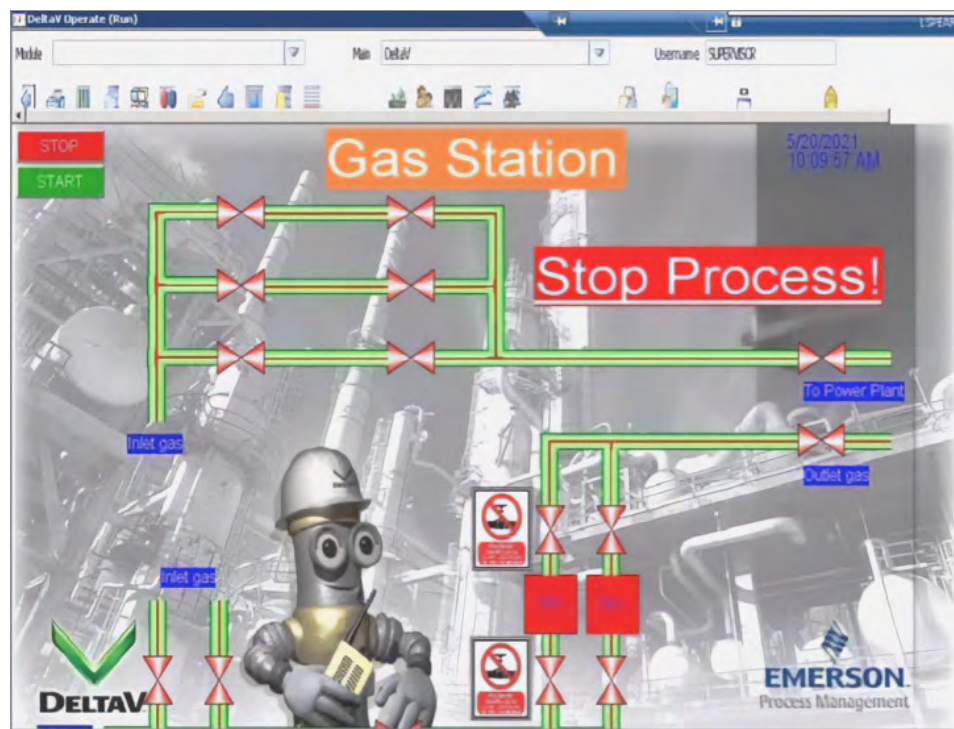


Рисунок 3. Газораспределительная станция за несколько секунд до взрыва

Последствиями реализации рисков на газораспределительной станции в реальной жизни могут стать человеческие жертвы, отставка руководства, судебные иски, ошибочные действия или бездействие персонала в случае чрезвычайной ситуации, поломка оборудования, затраты на восстановление, недополучение прибыли из-за простоя.

Выполняя анализ защищенности реальной инфраструктуры промышленного предприятия, эксперты по ИБ, скорее всего, смогли бы продемонстрировать лишь подмену данных о транспортировке газа в системе мониторинга. Провести атаки, нарушающие или останавливающие технологические или бизнес-процессы, им бы точно не позволили, а значит, и реализуемость рисков осталась бы под вопросом.

Какие риски ИБ актуальны для промышленных компаний

Анализируя защищенность инфраструктуры компаний, специалисты Positive Technologies ищут в ней уязвимые места и демонстрируют возможность проведения атак, моделируя действия хакеров. Наш опыт показывает, что уровень защищенности большинства промышленных компаний очень низок. Согласно нашим [исследованиям](#), главными уязвимостями являются:

- низкая защищенность внешнего периметра сети, доступного из интернета;
- низкая защищенность от проникновения в технологическую сеть;
- недостатки конфигурации устройств;
- недостатки сегментации сетей и фильтрации трафика;
- использование словарных паролей;
- использование устаревших версий ПО.

По результатам проектов по анализу защищенности в 2020 году было установлено, что в 91% промышленных организаций внешний злоумышленник может проникнуть в корпоративную сеть. Оказавшись во внутренней сети, он в 100% случаев может получить учетные данные пользователей и полный контроль над инфраструктурой, а в 69% — украсть конфиденциальные данные: информацию о партнерах и сотрудниках компании, почтовую переписку и внутреннюю документацию. Но самое важное, что в 75% промышленных компаний¹ был получен доступ в технологический сегмент сети. Это позволило злоумышленникам в 56% случаев получить доступ к системам управления технологическими процессами.

Статистика неутешительна, но попробуем разобраться, почему так происходит. Во внутренней сети каждой промышленной компании во время [проведения пилотных проектов по внедрению PT NAD](#) мы выявляем множество подозрительных событий.

Часть таких сетевых аномалий может говорить о возможной хакерской атаке.

PT NAD — это система глубокого анализа сетевого трафика (NTA) для выявления атак на периметре и внутри сети. PT NAD знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.

¹ По результатам 12 проектов по анализу защищенности корпоративных информационных систем от внешних и внутренних нарушителей в промышленных компаниях, реализованных в 2017–2020 годах, в которых установленной целью было получение доступа в технологическую сеть.

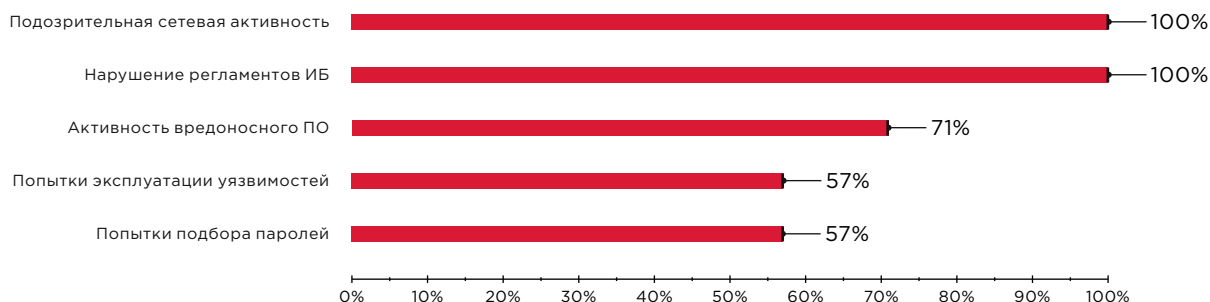


Рисунок 4. Угрозы ИБ в промышленных компаниях, реализованные в ходе пилотных проектов по внедрению PT NAD в 2020 году

Так, в одной промышленной организации PT NAD зафиксировал подключение по RDP к внешнему облачному хранилищу. На адрес этого хранилища по протоколам RDP и HTTPS в общей сложности было передано 23 ГБ данных.

Кроме того, в промышленности часто используется устаревшее ПО. По статистике, в последние годы количество уязвимостей в компонентах АСУ ТП неуклонно растет. Так, в 2020 году было выявлено на 25% больше уязвимостей, чем в 2019-м, преимущественно в энергетике, на производстве и водоочистных предприятиях. Дело в том, что работы по обновлению технологического оборудования требуется проводить во время специального технологического окна, а это всего несколько часов в неделю или даже в месяц.

Вектор атаки на критически важные системы может быть прост. Например, во время анализа защищенности одной промышленной компании эксперты Positive Technologies сначала проникли в корпоративную сеть и получили максимальные привилегии в домене. Затем собрали информацию об узлах технологической сети, получили схемы подключения оборудования АСУ ТП и обнаружили, что один компьютер связан с сетью АСУ ТП. Используя данный узел, специалисты смогли получить доступ в технологическую сеть.

Важно отметить распространенную ошибку администрирования таких компьютеров — сохранение параметров подключения (имени пользователя и пароля) в форме аутентификации удаленного доступа (например, по RDP). Злоумышленник, получив контроль над таким компьютером, может подключаться к ресурсам изолированного сегмента без учетных данных. Помимо этого, параметры подключения, адреса, схемы, пароли для доступа к системам в технологических сетях зачастую хранятся в открытом виде (например, в таблицах Excel) на компьютерах инженеров и других ответственных лиц.

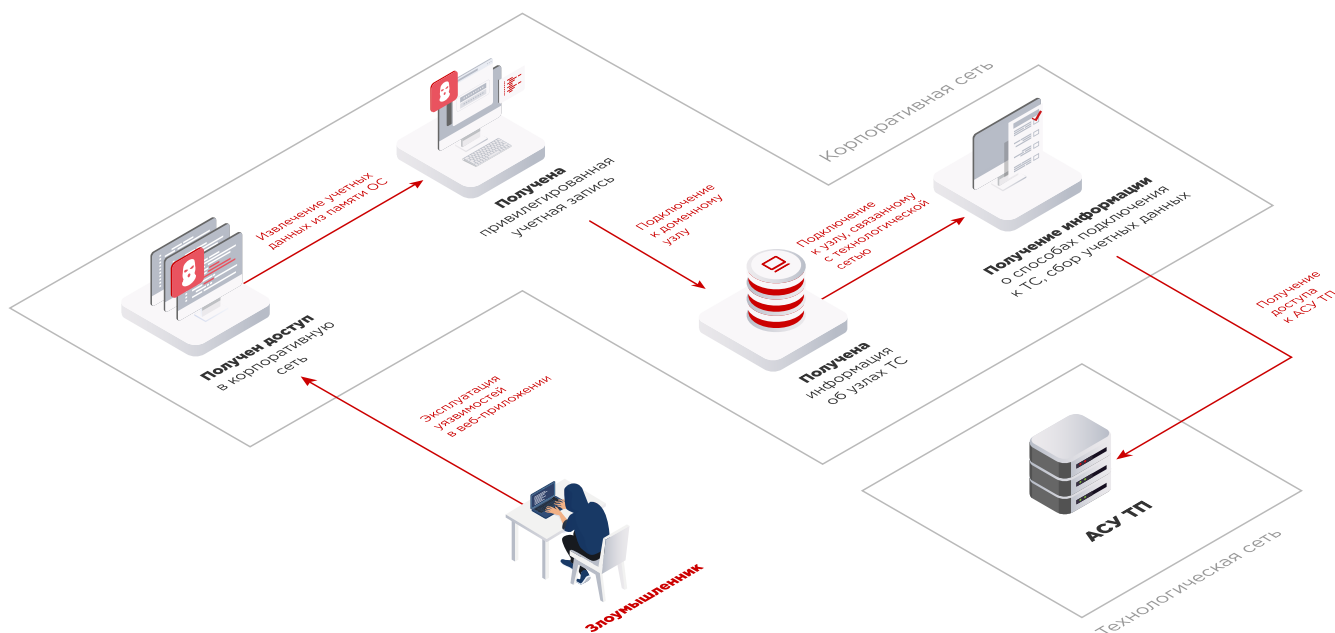


Рисунок 5. Вектор атаки на ресурсы технологической сети

Потенциальные риски, к которым может привести получение злоумышленником доступа к АСУ ТП, следующие:

- остановка производства,
- выход промышленного оборудования из строя,
- порча продукции,
- авария.

Однако проверить эти четыре риска ИБ в реальной инфраструктуре невозможно как раз из-за того, что это может негативно сказаться на технологических процессах.

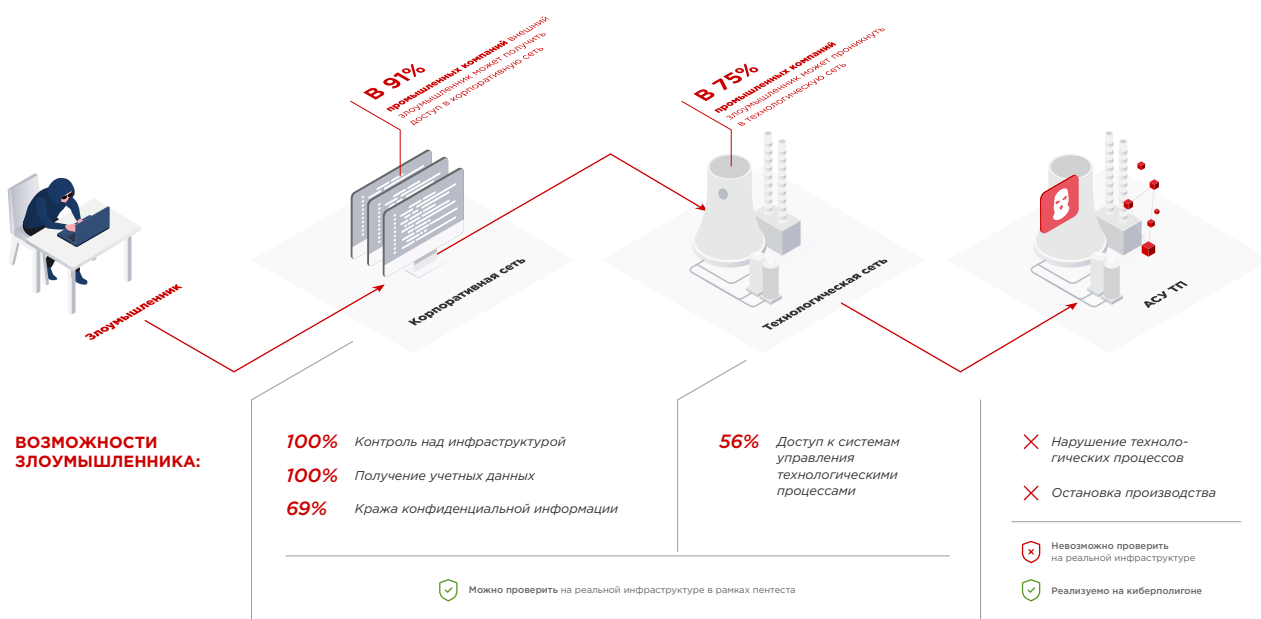


Рисунок 6. Результаты анализа защищенности промышленных компаний, выполненного экспертами Positive Technologies

Вывод, который напрашивается

Промышленность — это та сфера, которая в последние годы все больше интересует хакеров. Их атаки становятся все успешнее, а сценарии — сложнее. С другой стороны, предприятия далеко не всегда способны самостоятельно выявить целенаправленную кибератаку и на протяжении многих лет могут оставаться в иллюзии безопасности, рассматривая вероятность реализации киберрисков как минимальную. Хуже, если такие предприятия слепо уверены в надежности защитной автоматики и не проверяют эффективность защиты технологической инфраструктуры на практике. В то же время как результаты анализа защищенности показывают, что получить доступ к таким системам может быть просто.

В промышленной сфере, как нигде, требуется моделирование отдельных критически важных систем, позволяющее тестировать их параметры, проверять реализуемость бизнес-рисков, искать уязвимости.

Использование киберполигона для анализа защищенности производственных систем — это передовое решение, позволяющее корректно определить перечень недопустимых событий и последствия их реализации, а также оценить возможный ущерб, не нарушая при этом бизнес-процессы. Моделирование рисков на киберполигоне позволяет определить критерии их реализации — узнать условия, при которых хакер сможет атаковать, и к чему это приведет. Благодаря этому повышается эффективность и других работ по анализу защищенности компании. Кроме того, киберполигон — это место, где сотрудники служб информационной безопасности могут проверить свои навыки по выявлению инцидентов и реагированию на них.

Результаты моделирования рисков ИБ — это основа для принятия решений по усилению защищенности инфраструктуры компании от киберугроз.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/
PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](#).