Kaspersky Lab ICS CERT

KASPERSKY lab

Проблемы киберзащиты промышленных предприятий

Евгений Гончаров

05.12.2018 Version 1.0

Современные предприятия – энергетики, нефтехимии, металлургии, машиностроения, производства медикаментов, пищевой промышленности, транспорта, логистики и прочих отраслей – в своём стремительном развитии за прошедшее десятилетие перешагнули незримую черту, отделяющую физический мир машин и агрегатов от виртуального мира компьютерных программ, превратившись, по сути, в киберфизические системы, где объектами физического мира управляют инструкции машинного кода. Эти киберфизические системы строят с использованием современных IT-технологий и объединяют друг с другом и с внешним кибер-миром при помощи проводных и беспроводных каналов связи. Это многократно упрощает их эффективное использование и развитие, но одновременно делает их уязвимыми перед угрозой компьютерных атак.

Опасность, которую несет технологическому процессу и оборудованию внедрение киберфизических технологий, всё чаще признаётся и специалистами промышленных предприятий, и исследователями информационной безопасности, и государственными органами большинства стран. Однако решение задач киберзащиты промышленных предприятий, по признанию большинства вовлечённых в этот процесс или причастных к нему людей, происходит чрезвычайно медленно. Как правило, при этом приводятся различные причины и факторы, затрудняющие и замедляющие движение в направлении защиты промышленных объектов, либо вовсе препятствующие такому движению.

В данной статье мы обобщили наши знания и опыт, полученные на протяжении нескольких лет практической деятельности (выполнение аудитов безопасности и тестов на проникновение, расследование инцидентов, обнаружение и предотвращение атак, разработка и внедрение средств защиты, проведение тренингов для специалистов в области компьютерной безопасности и сотрудников промышленных организаций, участие в разработке рекомендаций и требований отраслевых регуляторов) и в общении с представителями промышленных предприятий, академических институтов и государственных учреждений различных стран.

Мы свели в общий список факторы, которые, на наш взгляд, оказывают сейчас и будут оказывать в обозримом будущем значительное влияние на ландшафт угроз, на разработку, внедрение и использование организационно-технических мер защиты объектов промышленности, и основные проблемы обеспечения киберзащиты промышленных предприятий, которые вряд ли удастся решить в ближайшее время.

Объективные факторы, влияющие на кибербезопасность промышленных предприятий

1. **Эволюция технологических процессов.**

   Необходимость производить новую, более сложную, продукцию изменяет требования к системам автоматизированного управления.

2. **Изменение процессов управления производством.**

   Подъём функций мониторинга и управления на более высокие уровни иерархии (от технологической установки внизу в кабинет главного инженера наверху и далее – в заоблачные выси промышленного интернета вещей и Индустрии 4.0).

3. **Постоянно возрастающая техническая сложность систем управления технологическим процессом.**

   Как следствие – переход на новые технологии при разработке систем автоматизированного управления, которые
   - разрабатываются зачастую третьей стороной;
   - заимствуются из IT;
   - используются большим количеством производителей.

4. **Уменьшение времени жизни систем управления.**

   С одной стороны, обновление средств автоматизации производства частично решает проблему необходимости поддерживать совместимость со старыми продуктами и системами при разработке и внедрении мер и средств защиты.

   С другой стороны, это приводит к уменьшению длительности цикла разработки и поддержки продуктов для АСУ ТП. С учётом постоянно увеличивающейся сложности разрабатываемых продуктов для систем автоматизированного управления, это накладывает дополнительные ограничения на возможные затраты для обнаружения и решения проблем кибербезопасности продуктов на стороне производителя.

5. **Повышение степени автоматизации, избавление от ручного труда.**

   - Рост общего количества систем автоматизации и прочих информационных систем на производстве.
   - Увеличение разнообразия информационных систем, разработка и внедрение новых, ранее не существовавших, типов систем.
   - Увеличение связности между системами.

6. **Укрупнение производств, покупки и слияния.**

   - Резкое увеличение разнообразия систем автоматизации при укрупнении и слиянии производств.
   - Внедрение новых систем и технологий, позволяющих унифицировать мониторинг и управление ранее несвязанными объектами и системами.
   - Поиск предприятиями наиболее подходящих решений для централизации систем мониторинга и управления технологическим процессом.
   - Увеличение количества поставщиков и подрядных организаций.
   - Усложнение вертикали управления и процессов принятия решений.

7. **Увеличение уровня защищённости «традиционных» жертв киберпреступников.**

   - Рост количества и качества используемых средств зашиты от традиционных атак, увеличение осведомлённости потенциальных жертв и зрелости процессов обеспечения безопасности.
   - Внедрение Managed Security от ведущих игроков рынка информационной безопасности делает высокую экспертизу в обнаружении и предотвращении атак более доступной для организаций и частных лиц – потенциальных целей злоумышленников.
   - Рост уровня экспертизы органов охраны правопорядка в области расследования киберпреступлений против домашних пользователей, компаний и организаций, таких как кража денег и выведение из строя IT-систем, делает традиционные кибератаки всё более рискованным видом нелегальной деятельности.
   - Как следствие всего вышесказанного, киберпреступники всё более настойчиво ищут новые, менее защищённые цели.

8. **Отсутствие очевидной повседневной угрозы – функциональной (технологическому процессу, оборудованию) и физической (людям и окружающей среде) безопасности, бизнесу промышленных организаций.**

   Многие промышленные предприятия и организации при планировании и ведении своей деятельности из всего многообразия возможных последствий кибератак учитывают только те, что потенциально ведут к уже смоделированным авариям с предварительно оцененным риском. Матрица этих рисков складывалась, как правило, под прессингом со стороны законодательно-нормативной базы и в условиях сложившейся во многих отраслях промышленности традиции.

   Определяющее воздействие на список рисков предприятия и конкретного подразделения внутри предприятия оказывает также разделение ответственности между вертикалями управления на одном предприятии и между предприятиями в отрасли. При этом, как правило, речь идёт об оценённых рисках возникновения критических ситуаций при случайном стечении негативных обстоятельств – исходя из теоретических обоснований и опыта практической эксплуатации оборудования.

   Объективно оценить вероятность кибератаки и, следовательно, соответствующие риски физических последствий кибератаки пока не представляется возможным – в том числе, по причине фундаментально не стохастической природы кибератак. Задача смоделировать все возможные последствия кибератак на промышленное предприятие на практике тоже пока оказывается не выполнимой. Таким образом, свести полностью планирование и реализацию организационно-технических мер киберзащиты к традиционным практикам функциональной и физической безопасности принципиально невозможно.

   К сожалению, эту реальность большинство промышленных организаций принять пока не могут или не хотят, и пытаются решать задачи оценки угрозы кибератак при помощи привычного аппарата псевдо-математической статистики. Если бы кибератак на промышленные организации было много, а их разнообразие было бы велико, если бы физические инциденты, вызванные кибератаками, были повседневной реальностью большинства предприятий, тогда, вероятно, можно было бы построить метрики и статистические модели, позволяющие дать хоть сколько-нибудь адекватные численные оценки угрозы. Тогда, вероятно, можно было бы пробовать использовать на практике методы оценки рисков применительно к каким-то угрозам или их составляющим. Сделать это сейчас – абсолютно невозможно по причине нехватки статистического материала по кибератакам и по их физическим последствиям.

Целевые атаки на системы автоматизированного управления всё ещё, к счастью, остаются экзотикой. Для большинства людей в промышленности перечень таких атак – это список несомненно тревожных, но крайне редких событий, на котором невозможно построить надёжную статистику.

Атаки, нацеленные на кражу денег, равно как и атаки вымогателей, хотя и становятся всё более частыми, пока обходят стороной значительную часть промышленных предприятий. Угроза таких атак часто остаётся недооценённой представителями промышленных организаций, которые с ними не сталкивались на личном опыте. Статистика предотвращенных попыток заражений промышленных систем автоматизации, которую мы публикуем на нашем сайте, явно свидетельствует о том, что системы технологической сети промышленных предприятий доступны для массовых атак и случайных заражений, и, следовательно, могут быть целями злоумышленников, рассчитывающих получить выкуп за разблокировку работы заблокированных ими систем. В самом деле, в 2017-2018 г.г. мы опубликовали несколько статей, рассказывающих об обнаруженных нами массовых вредоносных кампаниях, нацеленных на кражу денег в сотнях промышленных организаций в России и по всему миру (причём, именно промышленных, а не всех подряд, включая промышленные), что говорит о существенном увеличении такой угрозы.

9. Неохотное раскрытие информации об уязвимостях, атаках и инцидентах

Информация о проблемах информационной безопасности, обнаруженных уязвимостях, атаках и инцидентах во многих случаях считается конфиденциальной на всех уровнях экосистемы промышленного производства – производителями средств АСУ ТП, промышленными предприятиями, государственными структурами.

10. Геополитика

Государственные структуры оказывают постоянно усиливающееся влияние на безопасность промышленных предприятий. Это влияние может быть в различной степени как позитивным (повышение осведомлённости об угрозах, разработка и внедрение требований по защите объектов критической инфраструктуры, координация исправления уязвимостей, помощь в расследовании инцидентов), так и негативным (ограничение доступа к информации об инцидентах, ограничение доступа к технологиям защиты, прямая дезинформация, организация и проведение атак на предприятия и частных лиц как за пределами области юрисдикции государства, так и в её пределах). Действия государственных структур могут быть обусловлены как внутриполитическими, так и внешнеполитическими, в том числе, геополитическими факторами. Одно из важных последствий, к которым приводят обусловленные геополитическими интересами действия государств, – существенные изменения в системе доверия между производителями средств автоматизации, поставщиками услуг по их внедрению, производителями средств и поставщиками услуг защиты и потребителями в лице промышленных организаций. Этот всеобщий пересмотр уровней доверия, на наш взгляд, к сожалению, в большей степени играет на руку злоумышленникам, чем промышленным организациям, пытающимся от них защититься.

Проблемы кибербезопасности промышленных предприятий

1. **Постоянно растущее количество и разнообразие уязвимостей и угроз.**

   - Увеличение количества систем автоматизации и, как следствие, каналов управления и передачи информации, внутри технологического объекта и связывающих объект со внешним миром, в том числе, через интернет.
   - Появление каналов связи для мониторинга и телеуправления между ранее независимыми объектами.
   - Увеличение разнообразия средств автоматизации на предприятии увеличивает сложность и поддержки систем автоматизации, и обеспечения их безопасности.
   - Увеличение количества организаций и лиц, имеющих непосредственный или удалённый доступ к системам автоматизации, расширяет возможности злоумышленников при организации и проведении атак.

2. **Постоянно увеличивающийся интерес к промышленным организациям киберкриминала и спецслужб**

   - Падение уровня прибыльности и рост рисков, связанных с реализацией кибератак, нацеленных на традиционных жертв киберпреступников, толкает их на поиск новых жертв, в том числе, среди промышленных организаций.
   - Сложность структуры управления безопасностью и неотлаженность соответствующих коммуникаций, которые обусловлены, в первую очередь, особенностями вертикали управления промышленных предприятий и процессов принятия решений, делает промышленные предприятия более уязвимыми перед угрозой кибератак по сравнению с традиционными жертвами киберпреступников.
   - На руку киберпреступникам играют и особенности ведения хозяйственной и финансовой деятельности промышленных предприятий – система отложенных платежей, взаиморасчётов, нетривиальность бухгалтерии и прочие факторы, затрудняющие своевременное обнаружение факта кражи денег.
   - При организации атак на промышленные предприятия киберпреступники могут использовать в своих целях нежелание жертвы предавать огласке факт случившегося инцидента и нежелание обращаться за помощью к компаниям, специализирующимся на информационной безопасности, и в органы обеспечения правопорядка.
   - Ни для кого не секрет, что спецслужбы многих стран, равно как и другие организованные группы злоумышленников, действия которых обусловлены внутри- и внешнеполитическими интересами государств, финансовых и политических группировок, активно ведут исследования и разработку технических средств для реализации шпионских и террористических атак, нацеленных на промышленные предприятия. Исследователи информационной безопасности в своих расследованиях сложных атак и широкомасштабных вредоносных кампаний постоянно натыкаются на следы такой деятельности и артефакты, указывающие на такие группы злоумышленников. Приходится признать, что с учётом складывающихся геополитических реалий, равно как и с развитием средств автоматизации промышленных предприятий и переходом на новые процессы управления и модели ведения производственной и хозяйственной деятельности, эта ситуации продолжит развиваться в ближайшие годы в негативном для многих промышленных организаций направлении.

3. **Недооценка общего уровня угрозы**

Недостаток общедоступной информации о проблемах информационной безопасности промышленных предприятий, относительная редкость целевых атак, направленных на системы автоматизации, излишняя вера в системы противоаварийной защиты и неприятие объективной реальности (например, отрицание факта доступа в интернет или наличия случайных заражений компонентов АСУ ТП) сказываются негативно на оценке уровня угрозы владельцами и операторами промышленных предприятий и их персоналом.

4. **Неправильное понимание специфики угрозы и неоптимальный выбор средств защиты**

На протяжении десятилетий практические методы и технологии информационной безопасности развиваются как ответ на развитие технологий и тактик, применяемых в атаках на информационные системы домашних пользователей, офисных и телекоммуникационных сетей, поставщиков различных информационных услуг. Таким образом, технологии защиты как бы догоняют технологии нападения.

Хотя многие разработчики средств защиты и стараются работать на опережение злоумышленников, их разработки всё же опираются на знания, полученные в результате анализа большого количества реальных атак. Так, системы «Лаборатории Касперского» автоматически исследуют и обрабатывают более 300 000 новых экземпляров подозрительного
и вредоносного ПО ежедневно.

В мире промышленных предприятий и систем автоматизации технологического процесса сложилась уникальная ситуация, когда несколько громких инцидентов, к которым привели целевые атаки на очень ограниченное количество жертв, создали информационное поле, полностью сформировавшее представление о потенциальной угрозе – как среди исследователей информационной безопасности и разработчиков средств защиты, так и среди потенциальных пользователей этих средств.

К сожалению, публично доступная информация о многих из этих инцидентов была предоставлена только исследователями и разработчиками средств защиты от традиционных IT-угроз, сконцентрировавших свои усилия, в основном, на техническом анализе именно IT-составляющей соответствующих атак и не уделивших должного внимания анализу их OT- и киберфизической составляющей.

Получившиеся отчёты оказались, во-первых, слишком сложны для понимания большинством потенциальных пользователей средств защиты и, во-вторых, лишены важных с точки зрения OT деталей – об этом свидетельствуют многочисленные неверные толкования практически всех известных инцидентов, с которыми приходится постоянно сталкиваться в профессиональной среде инженеров.

Появившиеся в большом количестве производители новых специализированных средств защиты систем промышленной автоматизации (зачастую не имеющие достаточного практического опыта в разработке и применении средств защиты от традиционных IT-угроз), в отсутствии повседневной необходимости отражения атак, нацеленных на АСУ ТП и полевое оборудование, создали продукты, защищающие, возможно, не столько от реальных повседневных атак, сколько от синтетических сценариев, придуманных самими исследователями информационной безопасности иногда без опоры на практический опыт, а их активная маркетинговая деятельность сформировала спрос на такие продукты.

В то же время влияние перечисленных в предыдущих разделах факторов привело к тому, что системы автоматизации промышленных предприятий не только стали уязвимыми к случайным атакам не нацеленного специально на них вредоносного ПО, но и привлекли внимание традиционных киберпреступников к промышленным предприятиям, о чём свидетельствуют результаты наших исследований, опубликованных на портале ics-cert.kaspersky.com.

Таким образом, в индустрии сложилась опасная, на наш взгляд, ситуация, когда усилия и бюджеты производителей и потребителей средств кибербезопасности могут тратиться не на решение первоочередной задачи – защиту от реальных (и всё более частых) атак, – а на защиту от синтетических сценариев и атак воображаемого будущего, измышленного производителями средств защиты без исследования объективной картины ландшафта повседневных угроз.

5. Технические и организационные сложности защиты АСУ ТП.

О технических и организационных сложностях защиты промышленных предприятий написано и сказано очень многое. Если попытаться перечислить и проанализировать их все, получится фундаментальный труд, сильно выходящий за рамки данной статьи.

Мы перечислим лишь те проблемы, которые, на наш взгляд, наиболее сильно тормозят обеспечение кибербезопасности промышленных предприятий. Среди них есть как объективные, т.е. те, что обусловлены трудно преодолимыми факторами, так и проблемы, которые связаны с неправильной оценкой ситуации.

Среди важных задач, решение которых осложняется объективными факторами, нам хотелось бы прежде всего выделить следующие:

- Поддержка совместимости средств защиты с великим многообразием промышленных информационных систем и средств промышленной автоматизации, включая морально устаревшие, но всё ещё распространённые продукты и технологии.
- Внедрение современных процессов и практик SDL производителями систем промышленной автоматизации.
- Обязательное тестирование всех новых разрабатываемых средств АСУ ТП командами внешних исследователей безопасности и аттестация продуктов АСУ ТП к использованию на предприятиях с учётом требований безопасности и результатов прохождения внешних тестов.
- Обязательное обучение и аттестация инженеров и операторов промышленных предприятий кибергигиене и современным практикам защиты от кибератак.

Неправильной оценкой текущей ситуации, на наш взгляд, во многом обусловлены следующие проблемы:

- Выполнение требований пассивного характера работы средств защиты (работы только в режиме мониторинга) – данные об использовании продуктов «Лаборатории Касперского» в активном режиме на сотнях тысяч систем промышленной автоматизации по всему миру свидетельствуют об избыточности такого требования в подавляющем большинстве случаев.
- Выполнение требований тотальной сертификации / аттестации всех средств защиты производителями средств АСУ ТП. Требование значительно удорожает и усложняет разработку как средств защиты, так и продуктов АСУ ТП, при том что его выполнение, как правило, не даёт дополнительных гарантий беспроблемной совместной работы средств защиты и средств автоматизации.

Как показывает наша практика, на системах, владельцы или операторы которых требуют подобной аттестации, часто ими же установлено множество куда более потенциально проблемного ПО, чем средства защиты, и даже опасного ПО, для которого никто сертификатов на совместимость с системами АСУ ТП требовать при установке не стал.

Вероятнее всего, подобного рода проблемы исчезнут сами собой с течением времени – под возрастающим давлением атак злоумышленников. Однако, на сегодняшний день они зачастую становятся барьером к применению адекватных средств защиты, оставляя системы промышленной автоматизации уязвимыми к кибератакам.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab 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 lab ICS CERT

Ics-cert@kaspersky.com