Q&A
Вебинар по кибербезопасности от «Ростелеком» и Schneider Electric
Отвечает Андрей Иванов, технический консультант по кибербезопасности Schneider Electric

1. **Трехуровневая система АСУТП — сегодня это уже типичная структура для российских предприятий или большинство обходятся без них?**

Трехуровневая система АСУТП типична практически для всех типов предприятий. Да, могут быть дополнительные элементы, какие-то из них могут отсутствовать, но в целом это классическая пирамида управления предприятием. Обычно градация составных частей этой пирамиды выглядит следующим образом: датчики исполнительных устройств, программируемые логические контроллеры, SCADA-системы или АСУТП, NES-системы управления производством, и на самом верху расположены системы управления предприятием.

2. **По данным ФСТЭК, статистика категорирования объектов КИИ достаточно плачевна: от 1,5% до 50-60% по разным отраслям. При условии, что до 1 сентября 2020 года категорирование должно было быть завершено, в том числе и для предприятий промышленности. Какова ситуация с внедрением мер защиты в такой ситуации? Почему это происходит? В чём причина?**

На самом деле, причин может быть много. Во-первых, главенствует принцип: «Не спеши выполнять приказ, а то вдруг отменят». Когда были введены вышеупомянутые требования, стало понятно, что внедрение всех мер и средств защиты требует дополнительных расходов. Необходимо понимать, что в крупных компаниях бюджет на следующий год, как правило, формируется осенью. Во-вторых, следует учитывать финансовую составляющую. Зачастую крупные компании находится в ситуации, когда защита всех систем требует больших финансовых затрат, которые заложить в годовой бюджет невозможно. В связи с этим процесс идёт медленно.

3. **Многие объекты энергетик до сих пор аналоговые. Казалось бы, хорошо: что не оцифровано, нельзя взломать. Но всё же как защищать такие объекты?**

Существуют свои специфические меры защиты и естественно на аналоговые системы управления установить антивирус невозмжно. Однако это не отменяет защиту периметра, защиту на уровне физического доступа к этим системам управления и так далее. Согласно 239-ому приказу ФСТЭКа, если та или иная мера защиты не может быть применена, то, во-первых, это должно быть обосновано («нет компьютера – нет антивируса»); во-вторых, должны быть разработаны компенсирующие меры. В любом случае такие задачи решаются, разрабатываются определённые меры защиты. Дополнительно Минэнерго выпускает дополнительные требования к защите системы энергетики.

4. **Насколько внимательно малый и средний бизнес относится к обеспечению кибербезопасности своих предприятий, или пока этим озабочены преимущественно крупные компании?**

Естественно, в первую очередь этим вопросом озабочены крупные компаниии. Однако в течение 2020 года сформировалась тенденция, когда этому аспекту должное внимание уделяют малый и средний бизнес.

5. **Если представители малого и среднего бизнеса все же захотят обеспечить свои предприятия кибербезопасностью, то какую сумму они должны закладывать на это в своем годовом бюджете в процентном соотношении?**

Назвать точную цифру, к сожалению, невозможно по ряду причин. Однако цены на средства защиты есть в открытом доступе. Можно найти стоимость антивируса, межсетевых экранов и посчитать расходы самостоятельно. Для небольшого предприятия необходимы межсетевой экран, несколько лицензий на антивирусную программу, система резервного копирования. Также необходимо учесть привлечение сторонней организации, но, если бизнес будет выполнять работы своими силами, то общая стоимость проекта выйдет намного дешевле.

6. **Какие новые риски появятся с распространением в системах АСУТП мобильных устройств IoT и мобильных сетей передачи данных? Как в целом оценивается перспектива операторов сотовой связи на рынке АСУТП (услуги на базе LoRa, NBIOT, 4/5G)?**

Откровенно говоря, перспективы операторов сотовой связи оценить достаточно трудно. В своей работе мы не сталкивались с операторами как поставщиками средств защиты, а работали над организацией канала передачи данных между удалёнными площадками. Появление мобильных устройств в сетях АСУТП – отдельная тема для обсуждения. У этого вопроса два аспекта: первый заключается в том, что такие устройства получают все большее развитие. То есть планшеты и смартфоны используются для выполнения процедур обслуживания, контроля возможностей оборудования. Второй аспект — это дополнительные риски, связанные с безопасностью использования. Некоторые предприятия запрещают использование мобильных устройств в АСУТП. Однако существуют и такие, кто принимает на себя эти риски. В этом случае, естественно, должна быть обеспечена полноценная защита как таких устройств, так и каналов передачи данных между мобильными устройствами и основной информационной инфраструктурой.

7. **Во время общения с менеджерами по информационной безопасности обычно слышишь одну и ту же проблему: руководство не дает деньги на новые решения, связанные с ИБ. Скажите, как можно убедить начальство выделить деньги на эти цели? Тем более, что в так называемые "страшилки" уже никто не верит.**

Обычно презентации об информационной и кибербезопасности на профильных мероприятиях начинаются с этих самых «страшилок»: сколько атак, как они быстро растут, сколько угроз, сколько денег потеряно и так далее. На самом деле эти факторы можно найти в тех отчётах, примеры которых были продемонстрированы в ходе вебинара. Что делать с таким руководством? Однозначного ответа нет. Если руководитель считает это неважным, ненужным и не выделяет на это деньги, то вряд ли вы сможете что-то с этим сделать. Как показывает практика, это всё длится до тех пор, пока не случается реальный инцидент. Тогда сразу находятся и деньги, и возможности, начинаются разговоры с теми же менеджерами по информационной безопасности в духе «а почему вы меня раньше в этом не убедили».

8. **Можете рассказать, какие типичные ошибки совершает отечественный бизнес в вопросах кибербезопасности?**

Самая распространенная − отсутствие выделенного бюджета на запуск работы по внедрению средств защиты. Все последующие ошибки происходят именно по этим причинам. Как правило, всё упирается в финансовые средства и возможности их выделения из общего бюджета компании.

9. **Вы утверждаете, что даже оборудование, используемое для защиты, нуждается в защите. Аппетиты у всех растут: чем больше защиты и оборудования, тем больше нужно ресурсов для этого. Может ли этот**

защитный пузырь надуться до таких размеров, что в конце концов лопнет? Или это произойдёт не в ближайшей перспективе?

Если это и произойдёт, то, наверное, не в нашу эпоху. Второй момент: произойдёт ли – это отдельный вопрос. Исходя из истории и опыта развития как самих средств защиты, так и в общем, как правило, когда размер системы превышает определенный «некомфортный» уровень, то появляется что-то новое. К примеру, переход от релейной логики к программируемым контролерам: появились контроллеры, физические размеры системы управления сильно уменьшились, а их масштаб вырос. В будущем мы будем наблюдать те же процессы.

10. **Как пандемия отразилась на кибербезопасности?**

Пандемия очень сильно повлиляла на состяние кибербезопасости. Многих работников перевели на удалённую работу, и работодателям потребовалось организовывать удалённый доступ. С одной стороны, если раньше это было прямо запрещено, то с началом пандемии требования к удалённому доступу к объектам КИИ были значительно пересмотрены.

11. **Как предотвращать атаки методом "грубой силы"?**

Это уже не кибербезопасность, это − область деятельности служб безопасности предприятия, которые обеспечивают безопасность физическую: контрольно-пропускной режим на предприятии, в цехах и отделах, и, при необходимости, обеспечение вооружённой охраны.

12. **Вы говорили о том, что медицинские учреждения часто подвергаются атаке. Закон о телемедицине в России вступил в силу 1 января 2018 года. Как бы вы оценили сейчас защиту персональных данных в сфере телемедицины в России? Отлажено ли законодательное регулирование, нет ли дефицита компетентных сотрудников и оборудования в этой сфере? Есть ли еще какие-то проблемы, особенности?**

Я на этот вопрос ответить, к сожалению, не смогу, поскольку защита персональных данных – это немного другая область информационной безопасности, где существуют свои нормативные документы, регулирование и требования.

13. **Как понять, что именно стоит выбрать предприятию для организации своей ИБ: облачные или on-premise решения? Есть ли у вас в арсенале облачные решения?**

Облачные решения в арсенале компании есть, но выбор всегда остается за заказчиком. Требования ФСТЭК прямо прописывают, что если используются облачные решения, облачное хранение данных, то эти «облака» и data-центр должны обязательно находиться на территории России. У нас подобные решения в проработке, но пока предложить их, именно на территории России, мы не можем. Поэтому выбор остается за предприятием с учётом всех нормативных требований.

14. **Есть ли в вопросе безопасности промышленных объектов региональная специфика, если говорить о регионах России?**

Если честно, я не заметил, ведь требования существуют для всех. На региональном уровне эти требования никто не корректирует, делать это может только ФСТЭК. Это также могут делать руководители предприятия – через решения о применении к базовому набору каких-то дополнительных мер. Таким образом, в отношении региональной специфики особенностей я не вижу.

15. **Насколько высок дефицит кадров в сегменте кибербезопасности? Какие меры нужно предпринимать для его сокращения?**

Это больной вопрос. Дефицит кадров, наверное, есть сейчас везде, а в области информационной безопасности он существенный. До того же 1 января 2018, пока средства защиты для систем АСУТП были необязательны (но это не означало, что их не надо было внедрять), нормативных требований на уровне законов не существовало. Сейчас, когда было введено соответствующее законодательство и когда предприятиям потребовалось ему соответствовать, обнаружился дефицит кадров, поскольку пока такой необходимости не существовало, никто специалистов не привлекал, и никто их не готовил. Сейчас это очень острая проблема. Знаю, что сегодня ВУЗы стали предлагать программы обучения специалистов информационной безопасности, например, Российский государственный университет нефти и газа имени И. М. Губкина сформировал целый факультет по комплексной безопасности топливно-энергетического комплекса, где одним из направлений является кибербезопасность. Если говорить о профильном образовании, то существуют согласованные со ФСТЭК программы переподготовки, закончив которые можно занимать соответствующие должности в службе информационной безопасности.

16. **В Амурской области работают три ГЭС, космодром, строятся газовый завод и газохимический комбинат. Что теоретически могут «натворить» злоумышленники в области кибербезопасности на подобных объектах?**

Про космодром не скажу, поскольку не знаю, какие системы безопасности там используются. Ракету, наверное, они запустить не смогут, ведь нужно туда, как минимум, ее установить.

17. **Какое отношение Schneider Electric имеет к вопросам кибербезопасности? Каковы компетенции компании в этом вопросе?**

Компания имеет самое прямое отношение к вопросам кибербезопасности, потому что Schneider Electric является поставщиком систем АСУТП, систем энергоснабжения и, соответственно, должна предусматривать определённые меры защиты таких систем. Это касается всей нашей деятельности в мире и России, безусловно, с учётом нормативной базы и требований национальных регуляторов. В отношении мер по обеспечению средств защиты речь идёт о том, что это, во-первых, встроенный функционал безопасности, во-вторых – использование наложных средств защиты, но для того, чтобы они вместе (наложные средства защиты с нашими АСУТП) гарантированно могли работать, должно быть проведено определённое тестирование, потому что в ходе такого тестирования всплывают такие вещи, о которых не подозревал ни производитель, ни вендор АСУТП, ни вендор систем безопасности. Мы подобные тестирования ведём. В Иннополисе открыт Центр инноваций Schneider Electric – локальное российское подразделение, на базе которого мы ведём работу с вендорами средств защиты: проводим тестирование, выпускаем официальные документы о совместимости, вырабатываем типовые решения, какие настройки надо сделать при совместном использовании тех или иных средств и так далее. И у нас как российского юридического лица есть лицензия ФСТЭК на деятельность в сфере технической защиты конфиденциальной информации.

18. **Известны ли случаи полного уничтожения бизнеса в результате кибератаки?**

Полного, наверное, нет, не известны. Ущерб был причинён, но под полным уничтожением следует понимать, что компания закрылась или обанкротилась, однако, такие случае мне не известны.

19. **До 1 января 2024 года объекты КИИ должны перейти на использование отечественного ПО, до 1 января 2025 года - начать использовать**

преимущественно отечественное оборудование. На ваш взгляд, насколько это реальная задача и можно ли говорить о том, что к этим срокам российские разработчики и производители обеспечат рынок достаточно качественным софтом и железом, в том числе, с точки зрения кибербезопасности?

Можно сказать, что уже обеспечен – с точки зрения наличия программных средств, антивирусов. Российские вендоры предоставляют услуги по защите, мониторингу, своевременному информированию и предотвращению атак и так далее. С аппаратным обеспечением ситуация немного хуже. Те же российские межсетевые экраны существуют, но пока начального уровня, то есть если требуется высокая производительность, высокая пропускная способность, то межсетевой экран должен стоять на серьёзном канале передачи данных, и таких пока немного.

20. **Проводятся ли периодические проверки для выявления недостатков и соответствия безопасности уровню, требуемому для крупных компаний?**

Если учесть, что проверки проводятся и самими компаниями, то про все сказать не могу. Те компании, которые я знаю, безусловно, их проводят. Внедрение мер защиты всегда должно начинаться с инвентаризации того, что уже есть, что само по себе уже является проверкой. Если говорить о проверках компетентными органами, то ФСТЭК анонсировал первые проверки на соответствие требованиям КИИ в 2021 году. В планах заявлено 5 субъектов КИИ, но их наименования не разглашаются.

21. **Насколько высокую угрозу предприятиям несет миграция кадров по кибербезопасности? Насколько защищены компании в этой части и как можно удерживать кадры?**

Это вопрос к отделу кадров и к HR. О рисках буду говорить в отношении специалистов по информационной безопасности. Когда уходит человек, который знает, как устроена информационная безопасность на конкретном предприятии, это влечет определённые риски, особенно если человек ушёл чем-то недовольным. Как показывает практика, мир таких специалистов ввиду дефицита кадров достаточно тесный, и вряд ли человек, являясь серьёзным специалистом, будет вредить себе, передавая эту информацию хакерским группировкам для произведения атаки. Часто утечка подобной информации определяется очень быстро. После такого специалист про серьёзную работу на рынке информационной безопасности может забыть.

22. **Насколько сейчас вероятно повторение истории с вирусами WannaCry и Petya? Были ли вынесены из них нужные уроки?**

Естественно, они затронули и КИИ, поскольку в тех же АСУТП есть компоненты, которые используют компьютерные технологии, те же компьютеры и сервера. Это значит, что там есть те же операционные системы, на уязвимость которых и были рассчитаны эти вирусы, поэтому туда, где мер защиты не было или они оказались недостаточными, и попали данные шифровальщики. Уроки, безусловно, были вынесены. Особенно теми, кого это коснулось. Это как раз один из ответов на вопрос, про то, как заставить руководителей выделить бюджет. Пока гром не грянет…

23. **Может ли считаться объектом критической информационной инфраструктуры крупнейший в регионе музейный комплекс? Его ежедневно посещают сотни туристов и трудятся десятки сотрудников. Он оснащен всеми современными средствами информационной безопасности, а его повреждение может нанести серьезный урон науке и культуре РФ.**

С формальной точки зрения, нет, не относится. Дальше это уже решение руководителя, решение ответственных лиц, которые должны и обязаны предвидеть возможные

последствия выхода из строя каких-то инженерных систем, того же освещения, вентиляции, чего-то ещё. Кстати, в России не относятся к КИИ и предприятия пищевой промышленности.

24. **Защищён ли российский АПК? Поскольку объекты сельского хозяйства тоже отсутствуют в перечне КИИ**

Наверное, защищён, потому что там, где используются компьютерные технологии, так или иначе стоит обычный антивирус. Вопрос в том, в какой мере он защищён. Работая в области автоматизации, я сталкивался с объектами АПК. И когда там внедрялась система автоматизации, для неё прорабатывались меры защиты. В одной из крупных компаний, могу сказать точно, это было предусмотрено, причём это было лет 5 назад.

25. **Как бы вы оценили правовое регулирование кибербезопасности в России? Есть ли существенные пробелы?**

ФСТЭК – очень открытая организация, представители которой везде присутствуют и выступают на различных профильных конференциях, стараются на всё отвечать. И те пробелы, которые были выявлены за три года действия этого законодательства, ФСТЭК достаточно оперативно устраняет. К тому же приказу № 239 ФСТЭК было выпущено уже три обновления за последние три года.