Kaspersky ICS CERT

kaspersky

Модель зрелости безопасности интернета вещей: толчок к развитию безопасных систем

Екатерина Рудина
Евгений Гончаров

13.08.2019 Version 1.0

Оглавление

Разработка стратегии защиты от киберугроз – непростая задача, особенно для промышленных систем и интернета вещей. В процессах проектирования, разработки, интеграции, использования и сопровождения таких систем принимает участие большое количество сторон.

Оценка рисков, связанных с атаками, у разных участников отличается, при этом безопасность для бизнеса определенных игроков может быть как отрицательным стимулом (увеличение времени выхода на рынок для продукта из-за необходимости реализовать требования безопасности), так и положительным (безопасный продукт – это еще и конкурентное преимущество с точки зрения маркетинга).

В идеале выбор мер и средств обеспечения безопасности должен быть решением весьма сложной задачи оптимизации ресурсов компании, отвечать интересам бизнеса в условиях внешних и внутренних ограничений.

Цель модели зрелости безопасности интернета вещей (IIC IoT Security Maturity Model, IoT SMM) – обеспечить выбор способов защиты от киберугроз, которые соответствуют реальным бизнес-потребностям компании.

Модель зрелости безопасности интернета вещей равным образом может применяться к более или менее технологически сложным устройствам, компонентам IoT устройств и инфраструктур, и к самим инфраструктурам. Документ IoT Security Maturity Model: Practitioner's Guide содержит три примера применения этой модели зрелости: к промышленной линии пищевого производства с точки зрения системного интегратора, к шлюзу обновления ПО электронных блоков управления (ЭБУ) автомобиля с точки зрения поставщика автомобильных компонентов уровня tier-1 и к камерам видеонаблюдения в жилой зоне с точки зрения потребителя.

Почему и зачем нужна модель зрелости безопасности интернета вещей

«Игра в труса»

Основной проблемой разработки стратегии защиты от киберугроз для промышленных систем и интернета вещей является то обстоятельство, что чаще всего безопасность воспринимается бизнесом как предмет беспокойства и статья затрат. Именно поэтому обеспечение необходимых аспектов кибербезопасности и защиты от угроз часто становится коллективной «игрой в труса».[1]

Так, производители продуктов для автоматизации технологического процесса до сих пор пытаются переложить ответственность за обеспечение безопасности своих продуктов на клиентов, утверждая, что их продукт должен быть использован в изолированной (от интернета, от офисной сети и т.д.) среде. При этом они упорно игнорируют объективную реальность, в которой большинство предприятий в погоне за увеличением эффективности своей работы оказываются не в состоянии эти требования выполнить.

С другой стороны, мы нередко слышим от представителей предприятий различных отраслей, что они не могут (или не хотят) применить те или иные меры (установить патч ОС, например) и средства безопасности (установить антивирус) к своим системам промышленной автоматизации (например, рабочему месту оператора) без подтверждения со стороны производителя продукта. Таким образом представители предприятий стремятся хотя бы частично переложить ответственность за принятие решений по обеспечению безопасности на производителей используемых ими продуктов.

Поиск баланса бизнес-стимулов в случае безопасности приводит к стратегии «балансирования на грани».[2] Чтобы удержать равновесие, каждая из сторон – производители определенных видов оборудования, программного обеспечения, системные интеграторы, поставщики услуг, посредники, владельцы предприятий – ищут оптимальный набор мер безопасности и пытаются не выйти за рамки бюджета.

---

[1] Это не ругательство, а название одного из основных видов стратегических игр, которое восходит к игре в труса (chicken), в которую имели обыкновение играть американские подростки. Два подростка мчались навстречу друг другу на автомобилях. Тот, кто сворачивал в сторону, чтобы избежать столкновения, считался проигравшим (трусом), а тот, кто продолжал ехать прямо, побеждал. Более динамичный вариант игры рассматривается в реальном времени, когда решение меняется в каждый момент, и с течением времени риск постепенно повышается. Вариант коллективной игры с несколькими участниками еще более сложный.

[2] Тоже не просто красивое выражение, а вариант стратегии при динамической «игре в труса». Балансирование на грани (brinkmanship) – угроза, которая создает риск, но не неизбежность исхода игры, неблагоприятного для всех участников, если каждый игрок игнорирует пожелание в отношении своих действий и постепенно повышает риск до тех пор, пока один из игроков не уступит или пока не наступит неблагоприятный исход игры (в нашем случае – ущерб вследствие инцидента безопасности).

«Достаточная безопасность»

Оценка необходимости обеспечения безопасности у различных организаций будет всегда разной. Даже при схожих рисках последствия возможных инцидентов для одних компаний могут быть более значимыми, чем для других

В некоторых случаях кибератаки могут представлять существенную угрозу для организаций, даже если их прямой вины в инциденте нет. Например, компрометация оборудования крупного мирового производителя, размещённого в незащищенной сети его клиента, несет риски для этого производителя – хотя клиент мог попросту не выполнить рекомендации безопасности производителя, и оборудование могло быть не настроено безопасным образом. А для предприятия, отнесенного к КИИ, аварийные ситуации, вызванные кибератакой, недопустимы, даже если они обусловлены эксплуатацией незакрытых производителем уязвимостей.

Сама задача реализации «достаточно безопасной системы» может быть поставлена для различных участников цепочки производства, внедрения и использования систем промышленного интернета вещей по-разному. Вероятно, наиболее далёкими друг от друга бывают точки зрения производителя и потребителя.

Производителя интересует обеспечение безопасности только его продукта, зато он обязан учитывать всё многообразие условий его эксплуатации, ожидания и требования к нему со стороны всех клиентов. В наиболее общем виде у производителя основная цель по безопасности звучит так: минимальными усилиями сделать клиентов и потенциальных клиентов довольными безопасностью продукта.

Потребителя же безопасность того же самого продукта интересует не сама по себе, а в контексте её влияния на безопасность инфраструктуры, в которую этот продукт интегрирован. У потребителя основная цель по безопасности звучит так: получить продукт, который не ухудшит (а, в идеале, улучшит) безопасность его инфраструктуры.

При этом задачи обеспечения безопасности, в рамках которых рассматривается безопасность конкретного продукта, равно как и способы их решения для обеих сторон могут быть существенно разными. Чтобы пояснить эту мысль мы привели в Приложении развёрнутые примеры постановки задачи для двух гипотетических участников процесса обеспечения безопасности некого промышленного объекта – владельца (или оператора) объекта и производителя используемого на нём ПО или оборудования.

Цель модели зрелости безопасности интернета вещей

Правильный выбор мер и средств обеспечения безопасности не всегда очевиден. Более того, локальные бизнес-цели и мотивированные ими решения по безопасности, принимаемые различными участниками процесса обеспечения безопасности (например, производителем и потребителем ОТ-продуктов и услуг) могут оказаться не только разными, но и несовместными. Возможно самым неприятным аспектом этой ситуации является непонимание одной из сторон ограничений, потребностей и аргументов принятия решений по безопасности другой стороны.

Одной из целей разработки описываемой в статье модели стала попытка предложить некий общий знаменатель, задать систему координат, в которой решения по безопасности, принятые одной стороной, прозрачны и понятны для представителей другой стороны.

Далее в статье, чтобы избежать двусмысленностей, мы будем преимущественно рассматривать точку зрения производителя ПО и оборудования в ситуации выбора мер и способов обеспечения безопасности производимого продукта в его целевых применениях.

Конечная цель модели зрелости безопасности интернета вещей (IIC IoT Security Maturity Model, IoT SMM) – обеспечить соответствие способов защиты от киберугроз реальным бизнес-потребностям. Задача – сформировать конкретное описание состояния «достаточной безопасности» для системы, помочь ответственным за безопасность этой системы лицам сфокусироваться на наилучших способах достижения этого состояния и определить соответствующие меры защиты.

Зрелая с точки зрения безопасности система

Зрелая с точки зрения безопасности система характеризуется достаточным набором мер защиты, которые не влияют негативно на её функциональность. При этом определения «достаточности защиты» и понятия «негативно влиять на функциональность» для каждой системы свои.

Возникает вопрос: как именно производитель, скажем, сложного промышленного оборудования должен сделать выбор в пользу «достаточного» набора мер защиты с учетом специфичных характеристик, запросов и ограничений на реализацию этих мер?

На уровне бизнес-стейкхолдеров формируется запрос на «защиту оборудования от хакерских атак». Основная проблема в том, что представители бизнеса почти всегда не являются специалистами в области информационной безопасности. Уязвимость оборудования к атакам может быть, к примеру, обусловлена неудачной архитектурой ПО. В долгосрочной перспективе может рассматриваться дорогостоящий перевод оборудования на альтернативную, более устойчивую к атакам, платформу. Текущие версии также требуют технической поддержки и сопровождения, включая проверку на наличие уязвимостей и выпуск обновлений безопасности. Обратная связь с потребителем продуктов для получения информации об уязвимостях и инцидентах также требует содержания специализированного сервиса.

Для решения задачи выбора необходимых мер и средств защиты бизнесу требуется системный подход, который связывает приоритеты с целями безопасности и меры безопасности – непосредственно с ожидаемым эффектом. Поскольку способов сделать систему более безопасной (или компенсировать в достаточной степени ее небезопасность) довольно много, требуется эти способы упорядочить, чтобы можно было сделать выбор в пользу наиболее подходящих вариантов.

Роль архитектуры выбора

Сложность выбора стратегии защиты связана не столько с нахождением оптимального соотношения мер по критерию цена-эффективность, сколько с несовпадением нарратива, стоящего за определением этого оптимума, для различных заинтересованных сторон.

С учётом различий в бизнес-потребностях и в условиях недостаточной информации о возможных кибератаках и неясного влияния этих атак на функционирование системы, вендор и клиент (а также другие заинтересованные организации и лица, например, регуляторы) могут считать разные сценарии атак более вероятными и потенциально опасными, и различные практики защиты – более приоритетными для реализации.

Рассмотрим для примера возможные позиции гипотетических производителя ПО SCADA системы и его клиента.

В теории и клиент, и вендор заинтересованы получить безопасную by design систему, требующую минимальных затрат на поддержание её свойств безопасности. Однако часто такое желание разбивается о суровую реальность. ПО вендора содержит уязвимости, известные или ещё не найденные, оно развёрнуто в небезопасном окружении. Со временем появляются новые реализации атак, некоторые из которых могли быть не учтены на этапах разработки и внедрения продукта.

Оценка рисков, связанных с атаками, разнится на стороне вендора и клиента. Согласование приоритетов вендора и клиента, выбор мер защиты, полноты реализации этих мер и сроков реализации требует структурированного представления вариантов с возможностью хотя бы приблизительной оценки соотношения их эффективности и требуемых ресурсов, то есть архитектуры выбора.

Архитектура выбора – это систематизация вариантов, которая подталкивает людей к выбору способа действий и к началу этих действий, то есть в нашем случае – к созданию более безопасной системы.

Рассмотрим пример ситуации, когда в продукте вендора обнаруживается уязвимость.

В интересах клиента может быть немедленное исправление уязвимости патчем безопасности. Вендор же может медлить с выпуском патча, в силу целого ряда причин стараясь отложить исправление до выпуска следующей версии.

Для вендора выпуск патча – это отвлечение ресурсов от выпуска продукта, которого ждут на рынке. Патчем безопасности нового клиента не получить, а новой функциональностью продукта – можно. Работу над выпуском патчей никто не оплачивает, затраченные на нее ресурсы рассматриваются как убыток. Для многих вендоров выпуск патча несет еще и репутационный риск, так как в этом случае вендор официально заявляет о наличии ошибки. Выпуская патчи, вендор множит поддерживаемые версии продукта, что усугубляет проблему согласованности изменений в этих версиях. Этими факторами затраты тоже не ограничиваются – нужно поддерживать доставку патчей до клиентов теми способами, которые клиента устроят, и поддерживать осведомленность о необходимости обновления. Не выпуская патч, вендор откладывает работу до следующего релиза, когда либо актуальность проблемы станет меньше, либо можно будет одним исправлением решить сразу целый ворох проблем – а это экономия и на разработке, и на тестировании.

Возможна и обратная ситуация. В ряде случаев клиент может хотеть получать патчи в аккумулированном виде – как кумулятивные исправления или уже в составе новой версии продукта, который более эффективно решает его производственные и бизнес-задачи и в которой, к тому же, исправления безопасности будут сделаны более правильно и основательно. Ведь наладить процесс патч-менеджмента на предприятии – сложное и дорогое дело. Особенности реализации систем автоматизации и технологического процесса предприятий в ряде индустрий вообще не позволяют устанавливать патчи иначе как в редкие периоды остановки производства. Установка патча может потенциально грозить проблемами совместимости с окружением продукта в инфраструктуре клиента. И все такие обновления на стороне клиента должны в идеале проходить процедуру предварительного тестирования, которое не всегда возможно оперативно выполнить – по техническим причинам или даже ввиду формальных ограничений, обусловленных спецификой производства.

Не стоит думать, что в виде патчей всегда выпускаются только простые исправления, не затрагивающие основную функциональность или архитектуру продукта. Иногда исправление ошибки действительно требует архитектурных изменений – к сожалению, зачастую избежать этого оказывается просто невозможно.

Конечно, не стоит считать, что в новой версии продукта уязвимость будет обязательно исправлена каким-то иным, более правильным способом, чем при выпуске патча. Если ошибку можно исправить без архитектурных изменений (добавив проверки, изменив значения по умолчанию и / или внеся исправления в пользовательскую документацию), то её с большой вероятностью будут стараться исправлять точно так же и в следующей версии. Архитектурные изменения, как правило, вносят, только если нет другой технической возможности, или же они признаются более дешёвыми, чем последовательное исправление проблем, которые могут возникнуть в будущем при использовании существующей архитектуры.

В таких случаях уже нежелание клиента или невозможность для него своевременно исправлять уязвимости безопасности продукта может стать проблемой для вендора.

Поскольку даже в отношении такой, казалось бы, простой меры защиты как выпуск и установка патча изначальные позиции вендора и клиента могут существенно не совпадать, им нужно предложить такую стратегию выбора, которая приведёт их к согласованному решению.

Как работает модель зрелости безопасности интернета вещей

Иерархия практик обеспечения безопасности

Архитектурой выбора и ядром модели зрелости безопасности интернета вещей является иерархия практик обеспечения безопасности (security practices). Практикой обеспечения безопасности, к примеру, является реализация контроля доступа, защита данных при их хранении и передаче или управление обновлениями безопасности. Системный подход к выбору вариантов защиты поддерживается группированием практик по ожидаемому эффекту от их применения. Чтобы максимально упростить процесс выбора, на самом верхнем уровне группы практик объединяются в домены.

Три верхнеуровневых домена безопасности включают:

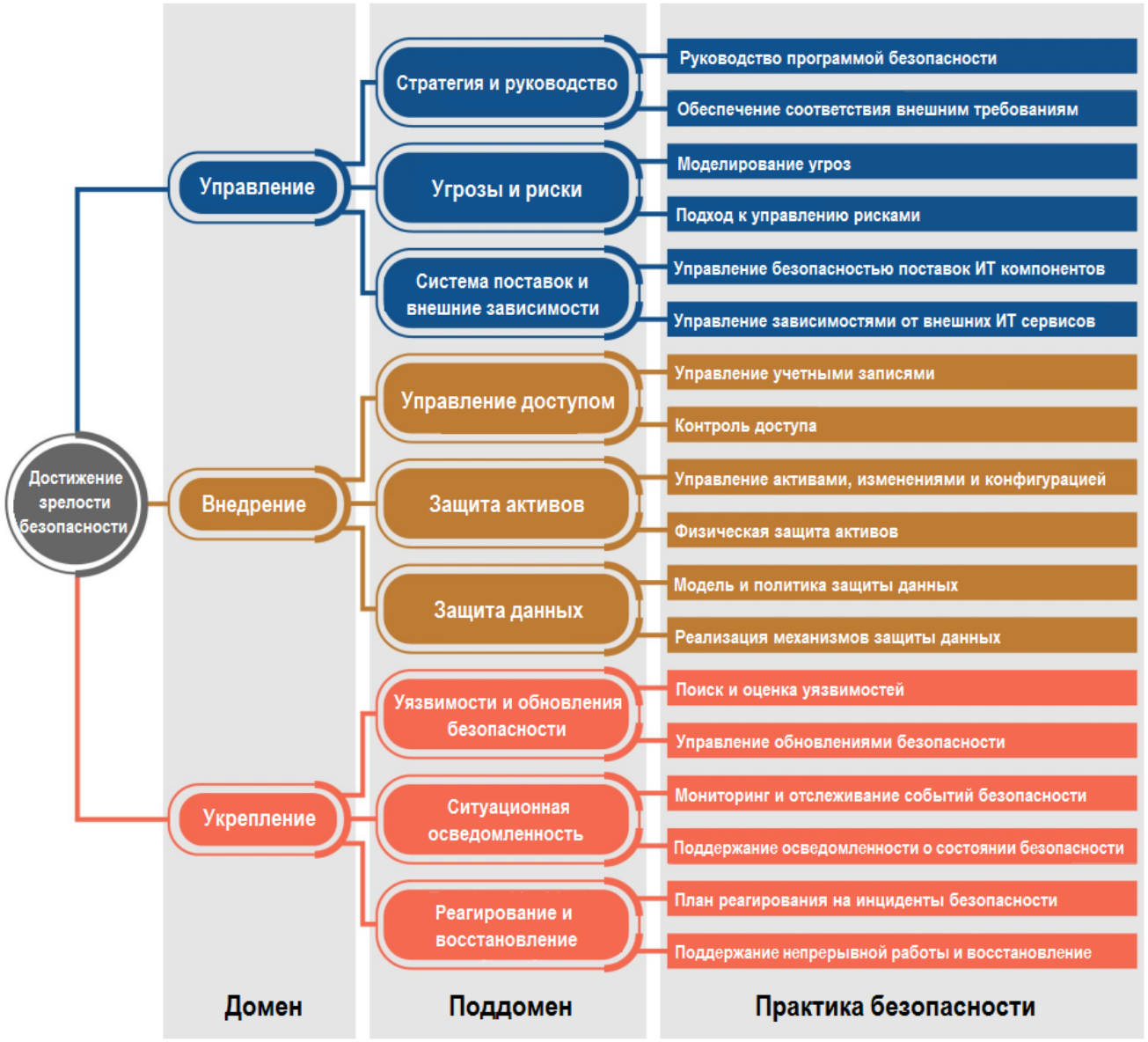
(1) управление безопасностью и организационные меры (Governance),
(2) обеспечение безопасности в силу конструкции (by design, Enablement)
(3) укрепление безопасности (Hardening).

Приоритет того или иного домена перед другим для вендора определяется потребностями бизнеса и особенностями системы (но первые – прежде вторых).

Название «архитектура выбора» для иерархии практик безопасности не означает, что выбор должен быть сделан в пользу единственной опции. Даже при наличии процедур по укреплению состояния безопасности нельзя оставлять системы небезопасными by design, и наоборот, любые системы должны предусматривать возможность реализации оперативных мер защиты. И в любом случае, организационные меры, будь то программа безопасности или политика безопасности для цепочки поставок, являются основой уверенности в эффективности технических мер. Меры из этих доменов также должны быть запланированы.

На втором уровне каждый из доменов делится на три поддомена, которые классифицируют практики безопасности в соответствии с проблемой, на решение которой они нацелены. И наконец, каждый поддомен ссылается на 2 практики, каждая из которых решает некоторую задачу. Пример: управление безопасностью (Governance) включает поддомен управления зависимостями (supply chain and dependencies management), который, в свою очередь, состоит из обеспечения безопасности цепочки

поставок (supply chain risk management) и управления зависимостями от подрядчиков, поставщиков сервисов и других сторонних субъектов (third party dependencies management) (см. рисунок).



Иерархия доменов, поддоменов и практик безопасности
Источник: IoT Security Maturity Model: Description and Intended Use White Paper

Как измерить зрелость безопасности

Чтобы устанавливать приоритеты и сравнивать реализацию мер безопасности, требуется шкала измерения. Оценивать эффективность метода защиты от киберугроз, перенесенного из классической IT-безопасности в среду интернета вещей, можно по двум параметрам. Первый – насколько сам подход хорошо реализован, насколько систематизировано его применение, так называемая полнота реализации (comprehensiveness). Этот параметр хорошо иллюстрируется на примере оценки

безопасности веб-приложений, к которой можно подходить с разной степенью усердия. Можно описать угрозы в общем – кража учетных данных, перебор пароля, DDoS атака. Это будет первый, минимальный уровень полноты (minimum). Можно проанализировать сценарии работы приложения для детализации модели угроз – второй уровень (ad hoc). Можно при детализации использовать систематизацию атак OWASP TOP 10, можно добавить к этому еще метод STRIDE, в этом случае уровень полноты – третий, упорядоченный (consistent). В конце концов, можно организовать целый формальный процесс периодической переоценки угроз, включающей все перечисленные методы – максимальный четвертый уровень (formalized).

Очень важно отметить, что полнота (comprehensiveness) – это еще не зрелость. Банковское веб-приложение требует наиболее полного подхода, а веб-приложение для сравнения текущего времени в разных часовых поясах может ограничиться рассмотрением сценариев работы с ним для выявления потенциальных проблем. Зрелый подход для приложения работы со временем будет недостаточным для банковского приложения. То есть зрелость, в отличие от полноты, – величина относительная.

Второй параметр, который имеет значение именно для интернета вещей, – насколько специфичным должен быть подход с учетом требований индустрии или даже конкретной системы. Оценка угроз для устройств, создаваемых, к примеру, в автомобильной индустрии (и многих других), должна фокусироваться на предотвращении в первую очередь физической опасности для жизни и здоровья людей, для окружающей среды. Значимые угрозы для медицинского устройства – те, что способны вызвать изменение специальных параметров его работы, иногда даже незначительное (например, дозировка лекарства для пациента). Смещение фокуса на специфичные проблемы (scope) для реализации конкретной практики безопасности также напрямую определяет ее зрелость, если мы говорим об интернете вещей. Здесь мы рассматриваем три варианта: общая неспецифичная реализация (General), специфичная для индустрии (Industry) и специфичная для системы (System). Последний вариант важен, поскольку сейчас появляется много решений на стыке индустрий, или просто специального назначения, из тех, что мы не видели раньше, – взять хотя бы «умный дом».

Таким образом, уровень зрелости определяется с учетом полноты реализации практики безопасности и специфики ее реализации для приложения интернета вещей. Каждое приложение (организация, система, отдельное решение) требует разной полноты и специфичности. Значит, и целевой уровень зрелости для разных приложений будет разным. Текущий уровень зрелости измеряется относительно ее целевого уровня, который задается профилем зрелости безопасности.

Что такое профили зрелости безопасности

Набор пар полнота+специфика (comprehensiveness+scope) по всем практикам безопасности называется профилем безопасности (Security Maturity Profile). Если такой набор определяет цели для конкретной системы, то он называется целевым профилем зрелости безопасности (Security Maturity Target). Это подробнейшим образом расписанные 36 параметров, по два на каждую практику. Чтобы получить их, нужно пройти несложную процедуру, последовательно определяя цели безопасности в рамках верхнеуровневых доменов, задачи для поддоменов и назначение практик безопасности на нижнем уровне иерархии. Картинка целевого профиля зрелости постепенно проступает в процессе анализа целей и задач обеспечения безопасности. Целевой профиль зрелости представляет собой описание стопроцентной зрелости безопасности для системы, к достижению которой следует стремиться при ее развитии.

В начале процесса описания целевого профиля зрелости безопасности на уровне бизнеса определяются приоритетные направления развития безопасности, связанные с верхнеуровневыми доменами. Далее установленные цели и связанные с ними уровни используются как умолчания (defaults), то есть базовые уровни полноты и специфичности, от которых технические специалисты отталкиваются в своих предложениях по реализации практик безопасности. Использование бизнес-приоритетов в качестве умолчаний для уровня полноты реализации мер защиты позволяет упростить процесс постановки задачи обеспечения безопасности. Соответствующая процедура описана в документе IoT Security Maturity Model: Practitioner's Guide.

Пример использования модели

Чтобы лучше объяснить, как используется модель зрелости безопасности интернета вещей для долговременного планирования задач обеспечения безопасности и расстановки приоритетов в реализации мер, приведем пример.

Рассмотрим систему управления отоплением, кондиционированием и вентиляцией на некотором предприятии. Система включает непосредственно управляющие контроллеры, системы SCADA, консоли человеко-машинного интерфейса, сети и системы связи. Консоли могут быть доступны извне для удаленного управления и быть в том числе точкой входа в систему для нарушителя, как это было в известной атаке на ритейлинговую сеть Target.

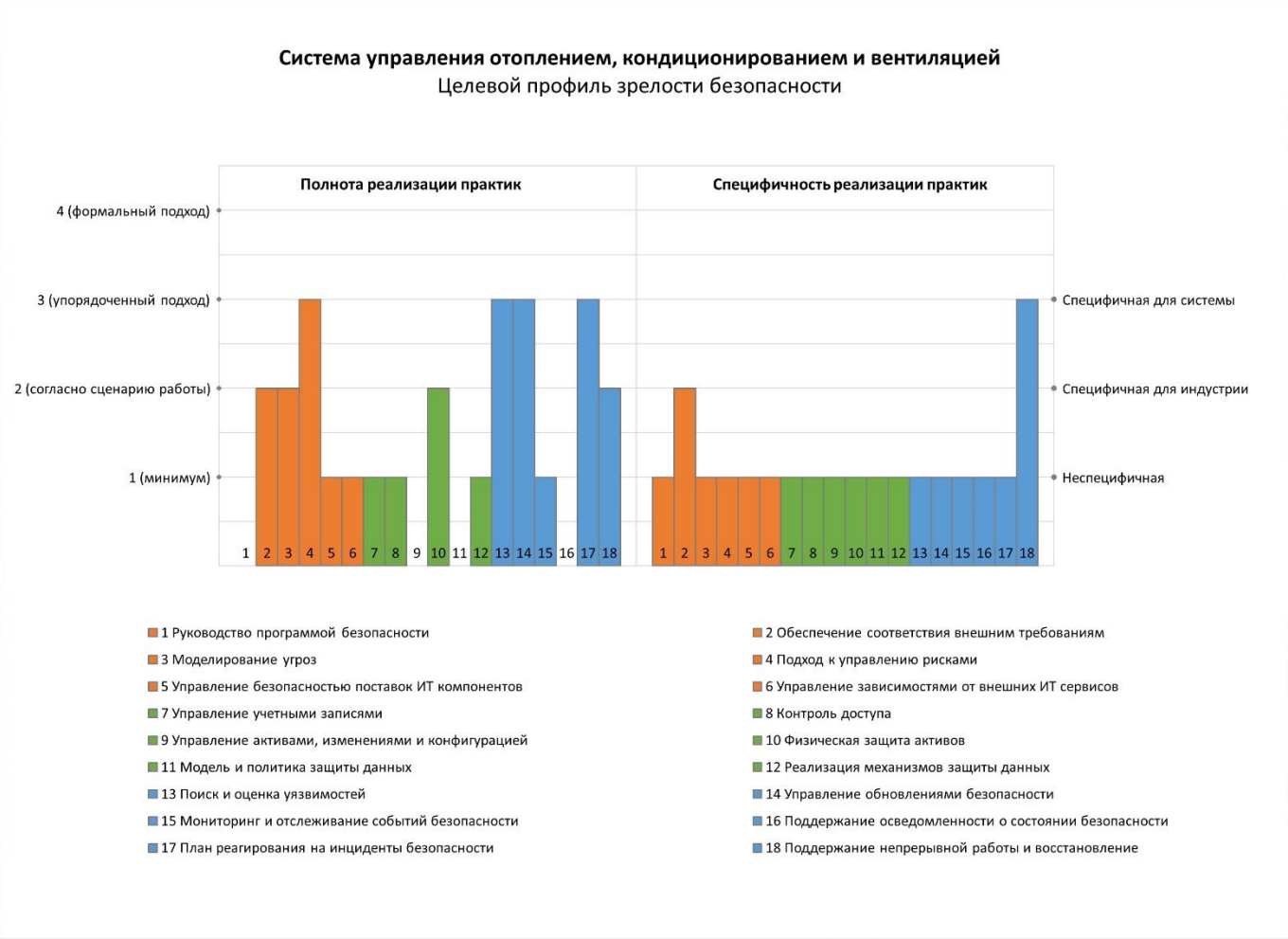
Объектом оценки зрелости безопасности может быть любой из компонентов или вся система в целом. Мы рассмотрим вкратце последний вариант.

С точки зрения системного интегратора, который непосредственно несет ответственность за работу системы, для уже функционирующей системы приоритетом является укрепление состояния ее безопасности. С этой целью проводится анализ уязвимостей, реализация управления обновлениями программного обеспечения и прошивок оборудования. Важный момент – реализация мониторинга (аудита) безопасности и внедрение политики реакции на инцидент, которая является частью общей политики предприятия. Чтобы обеспечить координирование этих практик, достаточное внимание уделяется управлению рисками (risk attitude). Все эти практики требуют продуманных методик и инструментов для их реализации (третьего уровня полноты или comprehensiveness). Такого же уровня гарантий требует поддержание непрерывности работы системы даже в условиях атак, ведь при нарушении работы системы HVAC, например, в результате DoS атаки, бизнес-риски могут быть

значительными. Обнаружение сбоя и последующее восстановление непрерывности реализуется специальным для системы образом, т.е. специфичным подходам к реализации практики (уровень специфичности – System) также нужно уделить внимание.

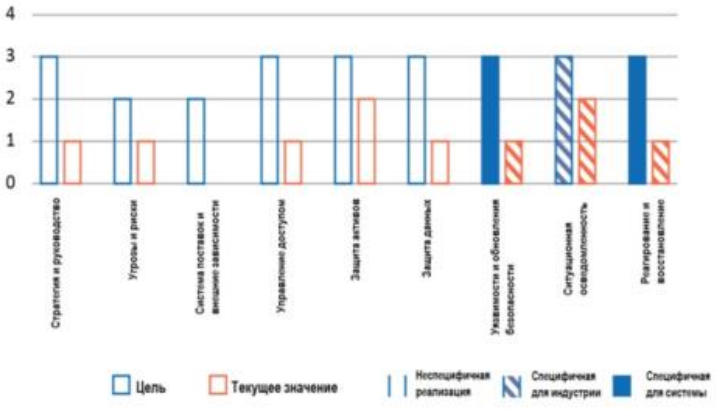
При этом интегратору также требуется анализ и моделирование угроз, определенный уровень гарантий, что атака не происходит со стороны подрядчиков, а также не является виной поставщиков, которые не хотят или не могут исправлять уязвимости в ПО или оборудовании своего производства. Эти практики, а также управление и контроль доступом к системам управления, реализуются в соответствии с общими сценариями работы системы и доступа к ней (второй уровень полноты или ad hoc). Также для отдельных компонентов требуется физическая защита. Прочие практики либо не требуются вовсе, либо реализуются на минимальном уровне. При реализации мер безопасности нужно убедиться, что система соответствует принятым в индустрии стандартам и требованиям, поэтому показатель compliance будет специфичен для индустрии.

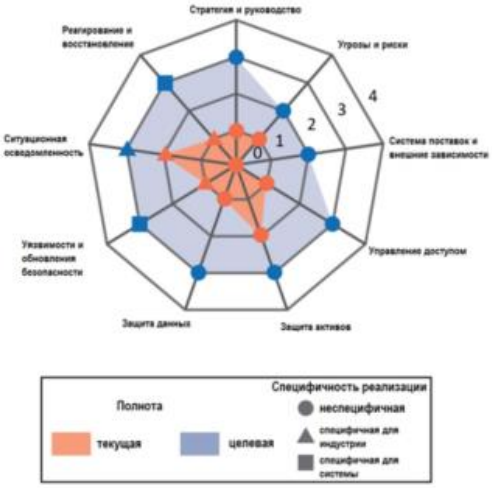
Суммируется целевой профиль зрелости безопасности в виде диаграммы, причем показатели полноты и специфичности практики оцениваются по отдельности.



Целевой профиль зрелости безопасности для системы управления отоплением, кондиционированием и вентиляцией

Помимо создания целевого профиля зрелости безопасности, для конкретной инсталляции системы мы можем оценить текущее состояние зрелости безопасности для системы и затем проанализировать расхождения текущего уровня с целевым. Визуализация расхождений может быть проведена на основе модных heat map или диаграмм типа «паутина», но самый удобный способ – при помощи по-разному заштрихованных столбчатых диаграмм, где штриховка показывает различия в показателе специфичности (scope) для каждой практики. На рисунке, взятом из IoT SMM White Paper, для простоты показана визуализация анализа расхождений на уровне поддоменов.





	Полнота		Специфичность		Анализ расхождений	
	Целевая	Текущая	Целевая	Текущая	Полнота	Специфичность
Стратегия и руководство	3	1	1	1		
Угрозы и риски	2	1	1	1		
Система поставок и внешние зависимости	2	0	1	1		
Управление доступом	3	1	1	1		
Защита активов	3	2	1	1		
Защита данных	3	1	1	1		
Уязвимости и обновления безопасности	3	1	3	2		
Ситуационная осведомленность	3	2	2	2		
Реагирование и восстановление	3	1	3	2		

Визуализация анализа расхождений текущего и целевого профиля зрелости безопасности
Источник: IoT Security Maturity Model: Description and Intended Use White Paper

Почему модель зрелости безопасности интернета вещей эффективна для принятия решений

Итоговая эффективность системы защиты определяется управленческими решениями, при принятии которых постоянно требуется делать выбор: какие средства использовать, насколько радикально подходить к изменению состава компонентов системы, на какие мероприятия тратить ресурсы. Этот выбор чрезвычайно сложен.

Важны два фактора: упрощение процесса планирования и организация согласований, поскольку видение приоритетов безопасности различается для заинтересованных в этой безопасности сторон. Структурирование практик позволяет упростить процесс планирования и принятия решений. Налаженный механизм общения между техническим персоналом и владельцами рисков со стороны бизнеса помогает согласованно подойти к этому планированию. Представители технической стороны смогут трезво обрисовать задачи и назначения практик безопасности, которые могут быть реализованы, их потенциальную эффективность относительно разных видов риска. Представители бизнеса, используя этот опыт, – приоритизировать меры обеспечения безопасности, поставить цели и построить кратковременные и долговременные планы по их достижению.

Эта задача долговременного планирования – экономическая, схожая с инвестированием, или выбором программы страхования, или любым другим упражнением с конфликтом стимулов. Современный подход к решению таких задач предусматривает использование так называемого nudge (подталкивания) – построения архитектуры выбора, поддерживающей эффективное принятие решений в определенной сфере. IoT SMM с установленным процессом формирования целевого профиля зрелости безопасности – это фреймворк для архитектуры выбора (или попросту nudge) в сфере информационной безопасности интернета вещей, который позволяет сделать первый шаг (а также второй, третий и так далее) в задаче построения безопасной системы, будь то крупное производство или фитнес-браслет.

Таким образом, использование модели зрелости позволяет оптимизировать постановку задачи безопасности интернета вещей, то есть определить уровень «достаточной безопасности», провести оценку и планирование объема работ, которые необходимо провести для её достижения с требуемой детализацией, начиная с уровня доменов безопасности вплоть до отдельных практик.

Может показаться, что использование модели зрелости безопасности для разумного подхода к выбору мер защиты или обоснованного отказа от них – это «выстрел в ногу» компании, которая занимается производством решений для обеспечения защиты от киберугроз и предоставлением соответствующих сервисов. Это не так. Доказано, что, измеряя намерения людей, можно повлиять на их поступки. Если задать людям вопрос об их намерениях, они с большей вероятностью поступят в соответствии со своим ответом. Модель зрелости безопасности интернета вещей как архитектура выбора подталкивает людей, принимающих решение о развитии бизнеса, в сторону использования защитных решений и задает вектор для более безопасного развития интернета вещей.

PS

Мы начали работать над моделью зрелости безопасности интернета вещей (IoT Security Maturity Model, IoT SMM) в рамках Industrial Internet Consortium (IIC) в марте 2017 года. До того времени подгруппа Security Applicability, которая в рамках консорциума занимается как раз вопросами применения практик безопасности к реальным приложениям интернета вещей, уже начинала смотреть в сторону модели зрелости – но реально подход, который сейчас описан в документах, появился именно тогда – весной 2017. Примерно через год вышел базовый документ IoT Security Maturity Model: Description and Intended Use (текущая версия доступна по ссылке). В феврале 2019 года вышло объемное руководство по применению модели IoT Security Maturity Model: Practitioners Guide (также доступен для скачивания). В настоящее время группа авторов работает над отдельными приложениями IoT SMM, а также над программой обучения ее использованию

Приложение.
Примеры постановки задачи обеспечения безопасности

В Приложении мы даем примеры постановки задачи обеспечения безопасности для двух придуманных нами участников процесса обеспечения безопасности некого промышленного объекта – владельца (или оператора) промышленного объекта и производителя используемого на нём ПО или оборудования. Подчеркнем, что данные примеры не являются универсальными, хотя мы и старались, чтобы придуманные нами владелец и производитель были достаточно типичными в своей категории. Мы надеемся, что развернутые примеры помогут участникам бизнеса лучше понять аргументы принятия решений по безопасности каждого из них.

Для компании-владельца или оператора промышленного объекта

- Определить потребность компании в повышении безопасности объекта.
  - Определить, насколько угрозы различного типа атак актуальны для предприятия:
    - Возможна ли угроза целенаправленной атаки со стороны спецслужб другого государства;
    - Могут ли системы предприятия быть интересны для киберкриминальных группировок;
    - Могут ли обычные преступники выиграть от использования кибер-средств для совершения преступных действий, нацеленных на активы предприятия;
    - Может ли атака на системы предприятия быть мотивирована заказом недобросовестных конкурентов;
    - Могут ли системы или сотрудники предприятия стать промежуточной целью атаки на партнёров / клиентов.
  - Определить масштаб возможных репутационных, финансовых потерь и юридические риски для компании и её сотрудников в случае успешной кибератаки на различные информационные системы и системы автоматизации объекта.
  - Определить набор необходимых к реализации требований по безопасности от регуляторов и оценить риски их невыполнения.
- Сформулировать цели безопасности, достижение которых необходимо для бесперебойного функционирования предприятия и получения запланированной прибыли.
  - Обеспечить выполнение обязательных требований регулятора.
  - Защитить наиболее важные для бизнес- и технологического процесса организации информационные системы и системы автоматизации от атак киберкриминальных группировок (с целью кражи денег или получения выкупа за разблокировку заблокированных систем).
  - Максимально защитить системы предприятия, необходимые для обеспечения безопасности сотрудников и защиты окружающей среды, от любых возможных воздействий со стороны потенциальных злоумышленников.
  - Защититься от юридических рисков, связанных с возможной недостаточной защитой от новых и технически сложных угроз, передав ответственность за обеспечение защиты третьей стороне (например, разработчику средств или поставщику услуг защиты).

    - Переложить финансовые риски, связанные с недостаточной защитой от выбранных типов угроз и реализацией всех остальных типов киберугроз, от которых защита не была предусмотрена, на третью сторону (например, на страховую компанию).
- Установить сроки реализации для каждой из сформулированных целей безопасности.
- Определить, какие ресурсы компания готова выделить на достижение поставленных целей безопасности, спланировать выделение ресурсов для достижения поставленных целей в заданные сроки.
- Выбрать процессы, меры и средства реализации сформулированных целей безопасности в установленные сроки с учётом спланированного выделения бюджета.
    - Провести инвентаризацию IT и OT активов организации.
    - Провести классификацию IT и OT систем с точки зрения их важности для бизнеса, безопасности процесса производства с учётом требований регуляторов.
    - Провести технический аудит состояния ИБ активов организации.
    - Организовать процесс анализа информации об уязвимостях IT и OT систем, процесс приоритизации исправлений безопасности и их своевременной установки.
    - Установить адекватные средства зашиты на все наиболее важные IT и OT системы предприятия.
    - Организовать своими силами или силами поставщика соответствующих услуг службу обнаружения и реагирования на инциденты ИБ.
    - Организовать процесс обучения сотрудников основам кибербезопасности.
    - Организовать процесс контроля выполнения поставщиками и подрядными организациями требований политики ИБ предприятия.
    - Организовать процесс тестирования и аттестации новых IT и OT систем перед их покупкой для нужд предприятия.
- Поскольку внедрение каждой из мер потребует дополнительных расходов в том или ином виде, определить приоритеты, дорожную карту внедрения выбранных мер и спланировать выделение ресурсов на каждую из мер.

Для производителя программного обеспечения и оборудования

- Определить потребность компании в повышении безопасности продукта:
    - Определить масштаб возможных репутационных и финансовых потерь в случае компрометации продукта при атаке на одного клиента; в случае масштабной атаки на многих клиентов. Очертить границу между приемлемым и неприемлемым риском.
    - Определить степень влияния требований по безопасности от регуляторов на основных территориях / рынках.
    - Определить, какие конкурентные преимущества может дать повышение безопасности разрабатываемого продукта и оценить потенциальную выгоду от их реализации.
- Сформулировать цели безопасности, достижение которых целесообразно для положительного влияния на продажи продукта.
    - Обеспечить достаточную степень доверия клиентов компании и продукту с точки зрения безопасности:
        - Защитить продукт от возможной компрометации в процессе его разработки и поставки (гарантировать безопасность процесса

разработки и поставки продукта, отсутствие возможности влияния на безопасность третьих сторон – поставщиков компонентов, дистрибьютеров, интеграторов);
        - Гарантировать безопасность данных пользователя / клиента – как на стороне продукта, так и на стороне инфраструктуры разработчика;
        - Продемонстрировать высокую скорость реакции на информацию о проблемах безопасности, обнаруженных в продукте (выпуск и доставка исправлений безопасности) или в инфраструктуре разработки / поставки продукта;
        - Продемонстрировать следование компанией-разработчиком лучших практик безопасной разработки продукта;
        - Продемонстрировать выполнение формальных требований регуляторов;
        - Пересмотреть маркетинговую политику, чтобы подсветить внимание, уделяемое компанией вопросам безопасности.
    - Оценивать текущее состояние безопасности продукта на стороне клиентов:
        - Отслеживать установку обновлений безопасности продукта;
        - Отслеживать появление информации об атаках на клиентов продукта;
        - Отслеживать информацию о появлении новых уязвимостей в окружении продукта на стороне клиента (например, в поддерживаемых ОС).
    - Помогать клиентам обеспечить безопасность в процессе эксплуатации ими продукта:
        - Снизить возможность использования продукта злоумышленниками для атак на системы и инфраструктуру заказчика (продукт не должен быть удобным инструментом в руках злоумышленников или слабым звеном в инфраструктуре клиента);
        - Повысить защиту продукта на стороне клиента от попыток его компрометации злоумышленником (продукт не должен быть лёгкой целью для злоумышленника);
        - Повысить степень информированности клиентов и партнёров (например, интеграторов, занимающихся внедрением и обслуживанием продукта) о потенциальных угрозах безопасности;
        - Помочь клиентам своевременно устанавливать обновления безопасности продукта;
        - Мотивировать клиентов устранять бреши безопасности инфраструктуры и окружения;
        - Предлагать профессиональные услуги по обеспечению безопасности клиентам.
- Установить сроки реализации для каждой из сформулированных целей безопасности.
- Определить, какие ресурсы компания готова выделить на достижение поставленных целей безопасности, спланировать выделение ресурсов для достижения поставленных целей в заданные сроки.
- Выбрать процессы, меры и средства реализации сформулированных целей безопасности в установленные сроки с учётом спланированного выделения бюджета.
    - Внедрить практику целенаправленного анализа угроз и постановки целей безопасности как часть процесса сбора и анализа требований ко всем новым продуктам и новым версиям существующих продуктов.
    - Внедрить процедуру анализа безопасности архитектуры при разработке продукта на стадии его проектирования и анализа влияния на безопасность

продукта всех предлагаемых архитектурных изменений в процессе развития и поддержки продукта.
    - Выделить позицию «архитектора безопасности», ответственного за принятие всех стратегических решений и архитектурных изменений, затрагивающих безопасность продукта.
    - При необходимости рассмотреть вопрос об архитектурных изменениях, повышающих устойчивость продукта к актуальным векторам атак.
    - При необходимости включить в продукт дополнительные технические средства обеспечения безопасности.
    - Внедрить практику статического и динамического анализа кода.
    - Внедрить практику обучения разработке безопасного кода всей команды разработки или ключевых её участников.
    - Организовать процесс внутреннего тестирования безопасности продукта как часть процесса разработки.
    - Выделить позицию «чемпиона по безопасности», ответственного за внедрение технических мер и средств проверки и обеспечения безопасности и принятие тактических решений по обеспечению безопасности продукта.
    - Организовать процесс тестирования продукта на безопасность силами внешней команды исследователей.
    - Организовать процесс сбора и анализа информации об обнаруженных в продукте уязвимостях.
    - Организовать процесс сбора и анализа информации об уязвимостях в используемых третьесторонних компонентах.
    - Организовать процесс оценки свойств безопасности третьесторонних компонентов при выборе реализации продукта.
    - Внедрить процесс постановки требований по безопасности (и контроля их выполнения) к поставщикам программных и аппаратных компонентов.
    - При необходимости рассмотреть вопрос о переходе на другие, более безопасные компоненты и сторонние технологии.
    - Для производителей оборудования – рассмотреть вопрос о переходе на более безопасную / устойчивую к атакам платформу (железо, ОС, runtime, и т.д.).
    - Организовать процесс сбора и анализа сведений об атаках, использующих слабости безопасности и уязвимости продукта, на клиентов.
    - Организовать процесс разработки и выпуска патчей безопасности.
    - Организовать процесс уведомления клиентов о найденных проблемах безопасности и их исправлениях.
    - Организовать процесс доставки исправлений безопасности до клиентов.
    - Внести изменения в PR- и маркетинговые стратегии компании – чтобы правильно подавать информацию о свойствах и проблемах безопасности продуктов.
    - Организовать процесс обучения по безопасности поставщиков и клиентов
    - Решить проблемы коммуникации с технологическими партнёрами и клиентами (для вендоров OEM-решений), иначе оценивающими нужность и значимость разглашения информации о проблемах безопасности.
- Учитывая, что каждая из мер потребует дополнительных расходов в том или ином виде – выделения дополнительных человеческих ресурсов, приобретения специальных автоматизированных средств анализа или покупку услуг у поставщиков услуг безопасности, – определить приоритеты, дорожную карту внедрения выбранных мер и спланировать выделение ресурсов на каждую из мер.

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

Kaspersky ICS CERT ics-cert@laspersky.com