МОДЕЛЬ КИБЕРУГРОЗ МПЦ

С.В. ГОРДЕЙЧИК,
заместитель технического директора ЗАО «Лаборатория Касперского»

Г.С. ГРИЦАЙ,
директор по безопасности промышленных систем управления Департамента исследований и разработки компании «Позитив Текнолоджис».

Д.С. БАРАНОВ,
директор по безопасности приложений

Модель киберугроз является одним из базовых инструментов, который используется при построении процессов информационной безопасности. На ее основе анализируется защищенность объекта, выбирается и анализируется эффективность средств защиты, разрабатываются методики и регламенты реагирования на инциденты.

Тем не менее трактовка этого довольно известного термина не всегда однозначна. Например, с одной стороны, согласно Методическим рекомендациям ФСБ России № 149/54-144 от 21.02.08 г. он означает перечень возможных угроз. С другой стороны, в ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» модель угроз определяется как физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Таким образом, модель киберугроз может быть представлена как в виде простого перечня угроз, так и в виде математической модели, которая может применяться при анализе защищенности, рисков нарушений кибербезопасности, выборе и обосновании средств защиты.

При разработке модели киберугроз ключевым является корректное описание объекта защиты. Попробуем выделить значимые с точки зрения модели киберугроз компоненты (функциональные модули) МПЦ, которые обладают собственными механизмами безопасности, являющимися определенным барьером (security boundary), осложняющим злоумышленнику реализацию атаки, и могут стать объектами атаки.

В большинстве случаев потенциальный злоумышленник стремится вмешаться в процесс управления ***напольными устройствами*** (стрелочными электроприводами, сигналами и др.). Тем не менее сами устройства не обладают достаточно развитыми интерфейсами управления, чтобы являться непосредственной целью атаки. Однако в случае применения системы радиоуправления ими она сама становится дополнительным объектом атаки, что должно быть учтено в модели киберугроз.

Центральный процессор (ЦП/ЦПУ), получая информацию от АРМов и других систем, обрабатывает ее и контролирует допустимость выполнения тех или иных команд в соответствии с поездной ситуацией и состоянием устройств ЖАТ. ЦП/ЦПУ, как правило, реализуется в виде специализированного программного обеспечения на основе стандартной операционной системы (ОС) и обеспечивает основные механизмы функциональной безопасности и отказоустойчивости МПЦ (дублирование вычислительных узлов, выявление и коррекция ошибок, контроль зависимостей). Это одна из приоритетных целей атакующего.

Модуль контроля зависимостей (МКЗ), как правило, является составным элементом ЦП/ ЦПУ и решает основные задачи контроля взаимозависимости стрелок и сигналов, выполнение требований безопасности движения поездов.

Объектные контроллеры (ОК) получают команды от центрального процессора, преобразуют их в управляющие сигналы, воздействующие на напольные устройства, и передают ЦП/ ЦПУ информацию о состоянии объектов управления. Они могут

частично выполнять задачи функциональной безопасности и контроля логических зависимостей. В зависимости от типа ОК могут быть одной из приоритетных целей атакующего, поскольку дают возможность воздействовать в обход системы контроля логических зависимостей, реализованной, как правило, на базе ЦП/ЦПУ.

Автоматизированные рабочие места (АРМы) оперативного и обслуживающего персонала выполняют роль человеко-машинного интерфейса HMI (Human Machine Inerface). В зависимости от назначения они позволяют следить за поездной ситуацией и состоянием устройств СЦБ, а также передавать команды на открытие сигналов, перевод стрелок и др.

Как правило, АРМы реализуются на основе персональных компьютеров (ПК) и операционных систем общего назначения (таких, как Windows) в виде специализированного программного обеспечения и могут обладать встроенными механизмами обеспечения безопасности. Они являются объектом с большой поверхностью атаки, поскольку обладают различными сетевыми и аппаратными интерфейсами (USB), а также активно взаимодействуют со всеми компонентами системы централизации и сотрудниками, что позволяет использовать векторы социальной инженерии* (воздействовать на операторов системы с использованием техники психологического манипулирования).

Сетевое оборудование (коммутаторы, маршрутизаторы, конвертеры, модемы, SIM-карты, точки беспроводного доступа и др.) обеспечивает взаимодействие между компонентами и может поддерживать как стандартные (Ethernet, IP, 802.11, 802.15, GSM и др.), так и специализированные или устаревшие протоколы (IEC 61158, Profinet, HDLC и др). Оно обладает достаточно серьезными вычислительными возможностями, средствами удаленного управления и др. Именно поэтому сетевые коммуникации являются одним из распространенных векторов атаки.

Сетевые протоколы обеспечивают взаимодействие различных компонентов МПЦ. При подготовке модели киберугроз следует учитывать не только транспортные протоколы (Ethernet, TCP/IP, HDLC, GSM и др.) и протоколы, реализующие логику МПЦ, но и вспомогательные протоколы, направленные на решение задач диагностики, удаленного управления, взаимодействия с операционными системами, системами управления безопасностью (СУБД) и др. Особенности и уязвимости этого компонента оказывают существенное влияние на возможность реализации тех или иных атак.

В МПЦ есть еще один важный компонент – различные по своей физической организации каналы связи (от токовой петли до беспроводных или магистральных каналов связи) для интеграции с другими системами. Это один из наиболее распространенных векторов реализации атак.

Интеграционные стыки и шлюзы (ИШ) с системами ЖАТ (ДЦ, ДК и др.) обеспечивают обмен информацией о состоянии устройств и поездной ситуации, а также управляющими командами со смежными системами. Они расширяют поверхность атаки, поскольку делают МПЦ частью распределенной системы. Как правило, требования по безопасности к системам ДЦ ниже, чем к МПЦ, что нельзя упускать из виду при их интеграции.

Следует также учитывать еще один значимый компонент в работе МПЦ – ***обслуживающий и оперативный персонал*** (электромеханики СЦБ, поездные диспетчеры, дежурные по станции, администраторы системы, сотрудники производителя, осуществляющие поддержку системы и др.). В этом случае могут применятся различные методы социальной инженерии. Общей чертой всех этих методов является введение в заблуждение с целью заставить человека совершить какое-либо действие, которое невыгодно ему, но необходимо социальному инженеру. При этом может использоваться целый ряд различных тактик: выдача себя за другое лицо, отвлечение внимания, нагнетание психологического напряжения и др.

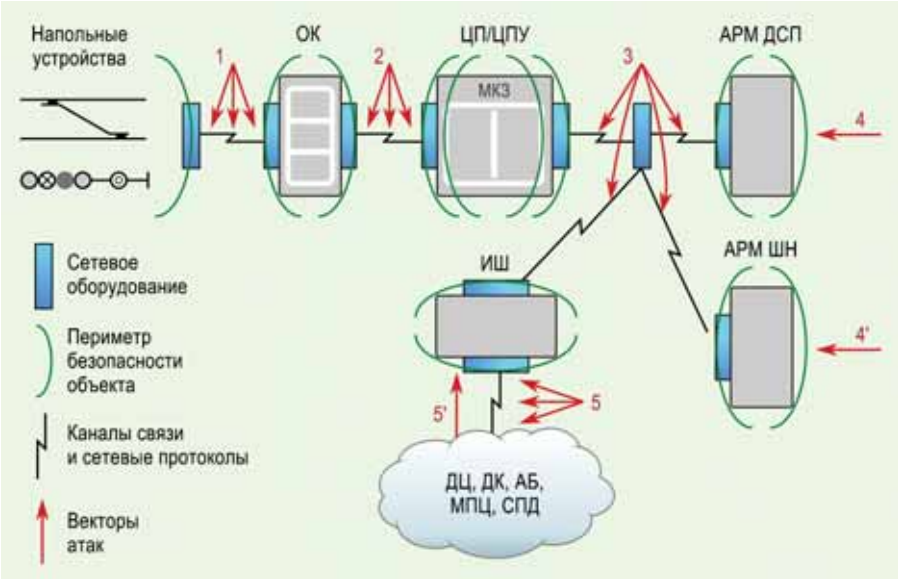
В большинстве случаев приведенная детализация достаточна для решения практических задач. Однако при более глубоком анализе (например, моделировании атак) следует учитывать, что многие из указанных компонентов не монолитны.

Так, например, ЦП/ЦПУ в основном состоит из нескольких логических блоков, использующих различные аппаратные ресурсы и экземпляры операционной системы. Обычно эти блоки реализуют механизмы отказоустойчивости и сравнения результатов с использованием мажоритарных схем, тестируют работоспособность и реализуют алгоритмы управления и центральных зависимостей. В этом случае ЦП/ЦПУ представляет собой многокомпонентную систему с ярко выраженными периметрами безопасности. Об этом следует помнить при создании модели киберугроз микропроцессорных систем управления.

Для построения корректной модели киберугроз необходимо определить векторы атак (доступа) – точки и цель воздействия потенциального злоумышленника на каждом из этапов проведения атаки. На рисунке показаны возможные векторы атаки на МПЦ, которая может быть реализована, как правило, при наличии какого-то внешнего интерфейса, позволяющего злоумышленнику воздействовать на свою цель.

Атаки могут быть реализованы локально или удаленно. Возможность проведения первой из них зачастую зависит от технической реализации интерфейса, через который она осуществляется. Так, например, для вектора 1 обычно учитывается локальный вектор, позволяющий злоумышленнику подать питание на светофор или стрелочный электропривод при физическом доступе к кабелю между ОК и напольными устройствами. Но в случае применения систем

* Социальная инженерия – метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека. В этом случае в роли объекта атаки выбирается не машина, а ее оператор.



радиоуправления напольными устройствами у злоумышленника появляется возможность удаленного воздействия.

Все показанные векторы атак позволяют косвенно учитывать вероятность реализации недекларированных возможностей (НДВ). В этом случае компонент, содержащий НДВ, обозначается скомпрометированным и сам становится интерфейсом для вектора угроз. Однако в случае если анализ наличия НДВ является одной из основных целей построения модели угроз, то объекты, которые могут содержать НДВ, должны обозначаться явно.

Существует три основных класса киберугроз МПСУ ЖАТ (см. «Кибербезопасность микропроцессорных устройств ЖАТ», «АСИ», 2015, № 4):

нарушение безопасности движения;

снижение эффективности процесса перевозок;

другие нарушения функциональной безопасности и надежности устройств.

Как правило, для их реализации требуется предпринять несколько атак с использованием уязвимостей и дефектов компонентов МПЦ. Рассмотрим примеры потенциальных цепочек атак, позволяющих реализовать угрозы различных типов.

Реализация угроз класса «Нарушение безопасности движения» через наиболее доступные векторы 4, 4′, 5, 5′ и 3 потребует от злоумышленника высокой квалификации для последовательного преодоления защитных механизмов ИШ, ЦП/ЦПУ, МКЗ и ОК. С одной стороны, ЦП/ЦПУ или МКЗ, как правило, реализуют механизмы контроля целостности и защиты от несанкционированного изменения логики расчета и контроля зависимостей, что дополнительно снижает вероятность успеха. С другой стороны, если не исключена возможность атаки через векторы 1 или 2 (путем манипуляции данными или проведения атаки «человек посередине» на каналы связи между напольными устройствами, ОК и ЦП/ЦПУ), то сделать это гораздо проще.

Снизить эффективность процесса перевозок можно, например, отобразив ложную поездную ситуацию на автоматизированном рабочем месте дежурного по станции через вектор 3 путем манипуляции сетевым протоколом между АРМ ДСП и ЦП/ЦПУ при наличии в этом протоколе соответствующих уязвимостей. Реализация этой угрозы через другие векторы потребует многоступенчатой атаки. Первым шагом может быть компрометация АРМ ДСП или АРМ ШН через векторы 4 либо ИШ через векторы 5 и 5′.

Нарушить функциональную безопасность и надежность устройств можно, в том числе путем временного вывода МПЦ из строя, реализовав атаку через векторы 4, 4′, 5, 5′ и 3. Для этого могут быть использованы уязвимости операционной системы АРМ ШН (например, неустановленные обновления безопасности или использование устаревших ОС Windows 2000/XP), прикладного ПО МПЦ, несложные пароли ОС и др. Еще каналы связи и сетевые протоколы можно атаковать путем снижения пропускной способности каналов связи (flood), внедрения ложных маршрутов (например, ARP Spoofing) и др. Большинство из этих атак реализуются с помощью вредоносного программного обеспечения общего назначения, ориентированного на заражение ОС Windows. Для атаки через вектор 4 и 4′ злоумышленник может воспользоваться векторами социальной инженерии, вынудив оператора подключить USB-накопитель с вредоносным ПО к АРМ или выполнить действия, выводящие систему из строя. Для реализации атаки через вектор 5 и 5′ злоумышленнику потребуется предварительно преодолеть защитные механизмы интеграционного шлюза, если такой компонент есть в системе и имеет встроенные функции безопасности.

В заключение следует сказать, что существуют различные уровни детализации модели угроз – от простого списка до математической модели. Предлагаемый подход моделирования угроз на основе модели МПСУ поможет определить наиболее вероятные векторы атак, противодействующие им защитные механизмы и узкие места системы с точки зрения кибербезопасности.

Использование миссиоцентрического подхода к анализу угроз МПСУ дает возможность отказаться от достаточно абстрактных показателей нарушения целостности, доступности и конфиденциальности, а также построить модель угроз исходя из требований безопасности движения, экономической эффективности и функциональной безопасности.

В случае применения методов математического и имитационного моделирования модель угроз может быть существенно расширена, что позволит оптимизировать анализ защищенности и рисков нарушений кибербезопасности, выбрать и обосновать набор используемых средств защиты.