ПРИНЦИПЫ ИНТЕГРАЦИИ ИНФОРМАЦИОННОЙ И ФИЗИЧЕСКОЙ МОДЕЛЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АТОМНОЙ СТАНЦИИ

Промыслов В.Г., Жарко Е.Ф., Семенков К.В.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
v1925@mail.ru, zharko@ipu.ru, semenkovk@mail.ru

Аннотация: При изучении и моделировании вопросов кибербезопасности следует учитывать и физическую, и информационную модели объекта. Гибридная модель, объединяющая информационную и физическую модели, является средством противодействия киберугрозам, а также средством оценки рисков кибербезопасности на стадиях проектирования и эксплуатации объекта.

Ключевые слова: кибербезопасность, моделирование, гибридная модель, АСУТП.

Введение

Применение цифровых систем и распределенной сетевой среды для реализации различных функций системы управления атомных станций (АЭС) приводит к появлению нового типа слабых мест в системах защиты и безопасности — так называемых киберугроз. Киберугроза — это умышленное воздействие на систему, которое, будучи реализованным, может оказать нежелательное влияние на информацию или технические средства автоматизированных систем управления технологическими процессами (АСУ ТП) [0]. Реализуемость киберугроз для АСУ ТП критически важных объектов, в частности, для АСУ ТП АЭС, подтверждена как реальными инцидентами кибербезопасности, так и экспериментами, проведенными организациями, ответственными за безопасность критических объектов [0].

Характерная особенность киберугроз АСУ ТП, отличающая их от чисто информационных угроз, состоит в следующем: в полной мере киберугрозы реализуются только посредством влияния на процессы, непосредственно происходящие на объекте управления, а цифровая среда является, в

основном, средой для переноса злонамеренного воздействия на АЭС. Эта особенность должна учитываться при проектировании архитектуры кибербезопасности и применении защитных мер.

Фундаментальные вопросы разработки архитектуры кибербезопасности критически важных объектов до настоящего времени полностью не решены, не разработаны сценарии применения математических и имитационных моделей для обеспечения кибербезопасности таких объектов не разработаны.

1 Формальные модели кибербезопасности

Процесс управления кибербезопасностью АСУ ТП АЭС в общем случае сводится к выполнению следующих шагов [0]: разработка политик и процедур безопасности; идентификация и классификация критических активов; назначение требований к мерам защиты и разграничениям прав доступа, которые определяют архитектуру кибербезопасности системы. Опыт обеспечения информационной безопасности показывает, что управление кибербезопасностью сложной системы невозможно осуществлять только на качественном, экспертном уровне и что необходимо иметь формальную (желательно, математическую) модель, описывающую политику безопасности системы.

Исследования по формальным моделям для чисто информационных систем тоже проводятся достаточно долго (например, в банковском и военном секторе), обзор некоторых известных моделей дан в работах [0,0]. В качестве таких моделей применяют либо вероятностные модели, либо детерминированные дискреционные модели.

Вероятностные модели безопасности, как правило, основаны на цепях Маркова, которые используются напрямую или реализуются посредством некоторого интерфейса; наиболее распространенным из интерфейсов стали сети Петри. Описывая состояние системы, модели подобного рода учитывают статистическую зависимость в использовании уязвимости в политике безопасности системы и характеристики уязвимостей отдельных компонентов системы. Для прикладных задач обычно используют однородную по времени модель, для которой применимы простые и эффективные численные методы решения. Представление поведения системы с помощью марковской модели требует определения всех возможных состояний системы и постоянных интенсивности перехода из одного состояния в другое. Результатами расчетов являются численные значения вероятности пребывания системы в данном наборе состояний. Марковские модели и их модификации широко используются при расчете надежности технических систем, имеется обширная методическая литература и опыт по их применению, но есть серьезные проблемы оценки информационной безопасности системы с их помощью, связанные прежде всего с трудностью получения достоверных входных данных для модели [0].

Следующий распространенный тип моделей безопасности — детерминированные дискреционные модели. Эти модели понятны большинству специалистов по информационной безопасности и содержатся в описании архитектуры безопасности системы и в программах и регламентах. Входные данные модели обычно включают в себя перечень активов в системе, а также наличие и тип связей между активами.

Формальные модели безопасности стали признанным средством повышения защищенности информационных систем, однако многие вопросы применения формальных моделей для АСУ ТП , а в особенности — АСУ ТП объектов критической инфраструктуры, требуют своего решения и исследований. В отличие от чисто информационных систем, на данный момент не существует общепризнанных формальных моделей безопасности АСУ ТП объектов критической инфраструктуры. Из-за особенностей политик кибербезопасности АСУ ТП прямое заимствование разработанных для банковской или военной сферы решений нецелесообразно [0], поэтому ведутся работы по адаптации информационных моделей для специфики систем управления технологическими объектами.

2 Построение гибридной модели кибербезопасности

Комплексная задача синтеза архитектуры кибербезопасности АСУ ТП АЭС состоит из решения нескольких частных задач, имеющих междисциплинарный характер, связанных как с информационной, так и физической структурой объекта. Исследования показывают, что для обеспечения кибербезопасности таких систем как АСУ ТП АЭС нельзя ограничиваться только информационными аспектами такой системы, необходимо учитывать аспекты технологической, физической безопасности, а в случае АЭС — и ядерной безопасности. Работы по согласованию этих аспектов для атомной энергетике представляются наиболее перспективными в свете достижения высокого уровня киберзащиты. Многие коллективы ведут теоретические и практические исследования в данном направлении, но проблема далека от решения.

Для описания соотношения различных аспектов кибербезопасности для АЭС: информационной, технологической, физической — используют модель, разработанную МАГАТЭ [0]. Модель задает общие рамки взаимодействия компонентов, но не определяет ни структуру данных, ни интерфейс между компонентами модели, что делает модель неполной и трудно применимой.

Мы полагаем, что исследовать АЭС как киберфизическую систему можно, работая с гибридной моделью системы. Под гибридной моделью мы понимаем совокупность информационной модели объекта, его физической модели и интерфейсов между этими моделями.

В качестве физической модели предлагаем использовать симулятор, гибкий моделирующий комплекс АЭС с водо-водяным реактором (ВВЭР) [0], настраиваемый на любой существующий или проектируемый энергоблок с реактором типа ВВЭР; в модели энергоблока заложена возможность оперативного изменения для учета изменений в технологическом оборудовании или системе управления энергоблоком. Данный комплекс построен по модульному принципу; технологическое оборудование сгруппировано, каждая группа описывается отдельным функциональным блоком. Функциональные модули существуют в нескольких вариантах исполнения, отличающихся полнотой и подробностью описания соответствующих объектов и процессов.

качестве информационной модели можно использовать интегрированную модель безопасности цифровой системы управления АЭС, задаваемую ее формальной моделью [0]. Данная модель представляет собой расширенную дискреционную модель передачи прав доступа, доработанную для АЭС, и использует теорию графов для описания отношений доступа между объектами и субъектами политики безопасности.

Для того, чтобы получить набор входных данных для информационной модели, необходимо идентифицировать цифровые активы и информационные связи между ними, т.е. фактически создать некий единый классификатор цифровых активов АЭС для модели. Однако само по себе наличие активов и связей между ними ничего не говорит о соответствии АСУ ТП принятой политике безопасности. Далее нужно принять некоторую политику безопасности, где задаются правила передачи информации системе, и в рамках принятой политики интегрировать классификатор активов в формальную модель и провести синтез архитектуры кибербезопасности, применив, например, метод, описанный в работе [0].

Ключевым элементом гибридной модели кибербезопасности является интерфейс обмена данными между информационной и физической моделью, который позволяет имитировать взаимодействие между АСУ ТП и физическим объектом и анализировать влияние кибернетических аномалий на АСУ ТП и физический объект. При этом должна быть решена задача интеграции измерений физических параметров АЭС в систему киберзащиты.

Для верификации системы должны быть разработаны шаблоны сценариев атаки на киберфизическую систему и типовые сценарии атаки.

Построенная на данных принципах гибридная модель киберфизической системы позволит верифицировать политики кибербезопасности и защитные меры, прогнозировать последствия кибератак различных типов и вырабывать способы противодействия киберугрозам.

Литература

1. *Полетыкин А.Г., Промыслов В.Г.* Формальная иерархическая модель безопасности верхнего уровня АСУ ТП АЭС // Ядерные измерительно-информационные технологии. 2012. Т. 4(44). С. 39-53.
2. *Van Dine A., Assante M., Stoutland P*. Outpacing Cyber Threats. Priorities for Cybersecurity at Nuclear Facilities // 2016.
3. https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf
4.International Electrotechnical Commission. IEC 62645 ed 1. Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем //2014
5. *Abraham S., Nair S.* Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains // Journal of Communications. Vol. 9. 2014, №. 12. . – P.899-907.
6. *Bishop M*. Computer Security. Art and Science. – Boston: Addison-Wesley, 2003. – 1136p.
7. *Kharchenko V., Butenko V., Odarushchenko O., et al.* Markov's Modeling of NPP I&C Reliability and Safety: Optimization of Tool-and-Technique Selection // Proceedings of 2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO). 2016, pp.328-336.
8. IAEA. IAEA NST 055 Handbook on the design of physical protection systems for nuclear material and nuclear facilities, (Draft). // August, 2017.
9. https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst055.pdf
10. *Жарко Е.Ф.* Гибкий моделирующий комплекс для систем поддержки оператора АЭС с реактором типа ВВЭР-1000 // Автоматика и телемеханика. 2006. Т. 5. С. 80-92.

11. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных станций // Проблемы управления. 2019. № 3. С. 61–71.