УДК 621.039.68

ОЦЕНКА ДОСТУПНОСТИ ЦИФРОВОЙ СИСТЕМЫ УПРАВЛЕНИЯ В ЗАДАЧЕ КИБЕРБЕЗОПАСНОСТИ

А.А. Байбулатов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: bajbulatov@mail.ru

В.Г. Промыслов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: v1925@mail.ru

Г.В. Промыслов
Государственное бюджетное общеобразовательное учреждение города Москвы «Школа № 171»
Россия, 119270, Москва, Доватора ул., 5/9
E-mail: georgypr@yahoo.com

Ключевые слова: кибербезопасность, доступность, время прохождения сигналов, АСУТП, АЭС, Network calculus.

Аннотация: Оценка кибербезопасности играет важную роль в обеспечении информационной и промышленной безопасности современных программно-технических комплексов. Среди всех свойств кибербезопасности для большей части систем управления и, в частности, для АСУТП АЭС наиболее важным считается свойство доступности. В работе предлагается оригинальный подход к оценке доступности цифровых информационных активов посредством расчета максимального времени прохождения сигналов с помощью теории детерминированных систем с очередями Network calculus. Представлены результаты исследования доступности модели IntServ под воздействием кибератак.

1. Введение

В последнее время много внимания уделяется обеспечению безопасности промышленных объектов и их систем управления. Поскольку большинство современных систем управления реализованы как распределенные цифровые программно-технические комплексы, особое значение приобретает кибербезопасность, которая непосредственно связана с цифровыми системами.

Обеспечение кибербезопасности означает защиту от кибератак, т.е. злонамеренных действий посредством цифровых средств, направленных на цифровые системы, обеспечивающие либо непосредственное управление, либо связь с системами управления. Обычно все кибератаки подразделяются на внутренние и внешние.

Для автоматизированных систем управления технологическими процессами (АСУТП) атомных электростанций (АЭС) кибербезопасность рассматривается как часть информационной безопасности [1] и характеризуется классической моделью,

объединяющей три свойства: конфиденциальность, целостность и доступность, каждое из которых обладает различной степенью ценности. Известно, что для атомной промышленности наиболее важным является свойство доступности [2]. Отсутствие доступности компонентов систем управления АЭС в результате кибератак может увеличивать вероятность серьезных нарушений и угрожать безопасности АЭС в целом.

Применяется много похожих определений понятия доступности. Мы будем придерживаться трактовки, в которой доступность интерпретируется как свойство, гарантирующее своевременный и надежный доступ к информации и функциям, относящимся к системе управления, и их использование [3]. В контексте данной работы доступность рассматривается как время обработки сигнала (прохождения сигнала от источника до приемника).

При нормальной эксплуатации АСУТП АЭС измерение времени прохождения сигналов является диагностической функцией и поэтому имеет отработанные способы реализации. Но, во-первых, некоторые состояния, например, критические, могут быть недоступны при нормальной эксплуатации. Во-вторых, из-за стохастического взаимодействия между компонентами системы измеряемый параметр приобретает вероятностный характер со сложным распределением. Поэтому прямые диагностические измерения не подходят для оценки доступности; для решения этой задачи необходим специальный метод.

При оценке доступности промышленных систем для моделирования внутренних атак на информационные активы применяются модели на основе сетей Петри [4]. Однако область применения аппарата сетей Петри ограничена. Главный его недостаток – это предположение об экспоненциальном распределении временных переходов, которое для ряда промышленных объектов, включая АСУТП АЭС, не может считаться приемлемым.

В работе представлен метод оценки доступности информационных активов АСУТП АЭС на основе аппарата Network calculus.

2. Оценка доступности информационных активов с помощью Network calculus

Теория детерминированных систем с очередями, известная как Network calculus, успешно применяется для решения задач расчета вычислительных сетей на протяжении последних 25 лет. Возникнув как альтернатива теории очередей, Network calculus предлагает прозрачный способ расчета показателей производительности как больших [5], так и локальных [6] компьютерных сетей. В настоящее время имеется целый ряд продуктов, основанных на Network calculus, как академического, так и промышленного назначения, включая критические объекты [7]. Network calculus становится достойной альтернативой теории очередей, особенно для объектов повышенного риска [8]. В отличие от сетей Петри Network calculus способен работать с более широким классом входящих потоков и позволяет вычислять максимальное время прохождения сигналов.

Network calculus предлагает удобную методику расчета времени прохождения сигналов в компьютерных сетях. Основные понятия, необходимые для решения этой задачи, следующие. Имеется система без потерь, рассматриваемая как черный ящик. Это может быть одиночный сервер, узел связи или целая сеть. Входящий и выходящий потоки моделируются кумулятивными функциями, т.е. суммарным количеством данных, наблюдаемых на входе и на выходе за определенный интервал времени. Поэтому время прохождения сигнала определяется как горизонтальное отклонение между этими функциями. Но максимальное значение времени прохождения сигнала может быть вычисле-

но с помощью соответствующих ограничений, а не фактических кумулятивных функций. Для этой цели используется верхняя граница или огибающая входящего потока и нижняя граница или минимальная функция обслуживания. При этом максимальное время прохождения сигнала равно горизонтальному отклонению между этими ограничениями [9].

Однако следует отметить, что вычисления, проводимые с помощью Network calculus, становятся прозрачными и удобными в применении только в случае линейных огибающих входящего потока и линейных функций обслуживания.

Что касается входящего потока, то широко используются две простые модели: «текущее ведро», которое задается аффинной функцией:

(1) $$E(t) = rt + b,$$

где r – скорость потока, b – «всплеск»;

и спецификация трафика (T-SPEC), которая предполагает огибающую вида:

(2) $$E(t) = \min\left(M + pt,\ rt + b\right),$$

где M – максимальный размер пакета, p – пиковая скорость, b – «всплеск», r – устойчивая скорость, $M \le b$, $r \le p$.

Функции обслуживания реальных устройств вычислительных сетей (серверов, коммутаторов, шлюзов, и т.д.) в большинстве случаев определяются функцией следующего вида [9]:

(3) $$S(t) = \begin{cases} R(t-T),\ t > T \\ 0,\ t \le T \end{cases},$$

где R – скорость обслуживания, T – задержка обслуживания.

Для системы с входящим потоком (1) и функцией обслуживания (3) максимальное время прохождения сигналов [9]:

(4) $$d = \frac{b}{R} + T,\ r \le R.$$

Для системы с входящим потоком (2) и функцией обслуживания (3) (это стандартная модель интегрированного обслуживания, IntServ) максимальное время прохождения сигналов [9]:

(5) $$d = \frac{1}{R}\left[M + \frac{b-M}{p-r}\left(p-R\right)^{+} \right] + T,\ r \le R.$$

Как показывает практика [6], многие реальные системы АСУТП могут быть описаны с некоторым приближением моделью (1), (3) или (2), (3). Поэтому возможно получить значение максимального времени прохождения сигналов между активами (4) или (5) и использовать его для оценки доступности. Изменяя различные параметры модели и рассчитывая максимальное время прохождения сигналов, можно анализировать киберустойчивость системы к изменению отдельных параметров как самой системы, так и внешних условий, где киберустойчивость определяет, насколько система остается доступной во время кибератаки на нее и после прекращения кибератаки [10].

Рассмотрим, например, стандартную модель IntServ и исследуем, как максимальное время прохождения сигналов (5) зависит от параметров входящего потока (2) и функции обслуживания (3). Будем считать, что эти параметры изменяются под влиянием кибератак: внутренние атаки воздействуют на функцию обслуживания, а внешние – на входящий поток.

Рассмотрим в качестве примера внешней атаки атаку типа отказа в обслуживании (Denial of Service, DoS). Для атаки внешний нарушитель должен получить доступ к входному каналу связи атакуемой системы и варьировать параметры входящего потока (2) таким образом, чтобы существенно изменить временные характеристики системы.

Зависимость максимального времени прохождения сигналов d от параметров входящего потока: «всплеска» b и пиковой скорости p и фиксированных остальных характеристиках системы приведена на рис. 1. Можно видеть, что зависимость имеет пороговое значение при $p = R$. Если $p \le R$, то максимальное время прохождения сигналов d постоянно и не зависит от изменения параметров. Если $p > R$, то $d \sim bp^x$, где $-1 < x < 1$; в случае $p \to \infty,\ b \to \infty$, что обычно происходит при DoS атаках, $d \sim b$.

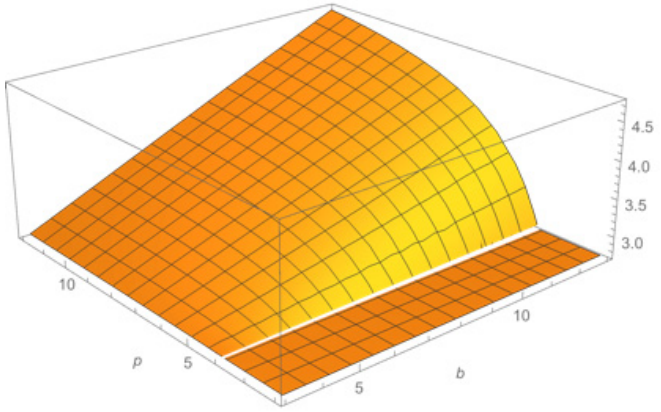

Рис. 1. Зависимость максимального времени прохождения сигналов d от параметров входящего потока: «всплеска» b и пиковой скорости p.

Исследуя зависимость максимального времени прохождения сигналов d от других параметров входящего потока: максимального размера пакета M и устойчивой скорости r и фиксированных остальных характеристиках, можно видеть, что $d \sim M + \frac{M}{r}$. Если $M \to \infty,\ r \to \infty$, то $d \sim M$.

Рассмотрим внутреннюю атаку. Внутренний нарушитель может влиять на характеристики сервера, обрабатывающего входную информацию, например, запуская параллельную программу и занимая процессор. Исследуя зависимость максимального времени прохождения сигналов d от параметров сервера: скорости обслуживания R и задержки обслуживания T и фиксированных остальных характеристиках, можно заключить, что если $R \ge p$, то $d \sim \frac{1}{R} + T$; если $0 \le R \le p$, то $d \sim T$ и мало зависит от уменьшения R, т.е. только после некоторого порогового значения R система будет терять свою доступность.

3. Заключение

Представленная работа посвящена одному из свойств кибербезопасности – доступности, для оценки которой выбран оригинальный показатель – максимальное время прохождения сигналов от источника до приемника; рассчитывается этот показатель с помощью теории детерминированных систем с очередями Network calculus. Показано, что, изменяя различные параметры модели, можно оценить доступность системы и ее поведение при атаках внутреннего и внешнего нарушителя (типа DoS атак).

В качестве примера проанализирована система управления, описываемая моделью IntServ, и найдено, как кибератаки и соответствующие изменения параметров входяще-

го потока и обслуживания влияют на максимальное время прохождения сигналов и, следовательно, на доступность.

В результате исследования показано, что доступность информационных активов по-разному зависит от изменения различных параметров модели, что необходимо учитывать при анализе влияния кибератак на кибербезопасность.

Результаты, представленные в работе, основаны на деятельности по проектированию и эксплуатации АСУТП АЭС, но они могут быть также успешно применены для систем управления других промышленных объектов.

Дальнейшее развитие представленной темы исследования возможно в части применения предложенного подхода к более сложным системам, чем рассмотренные простые модели.

Список литературы

1. Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев М.Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций // Проблемы управления. 2018. № 3.С. 47-55.
2. IEC 62645:2014. Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems. Edition 1. IEC, 2014. 43 p.
3. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности. М.: Стандартинформ, 2016. 62 + vii с.
4. Nasr P.M., Varjani A.Y. Petri net model of insider attacks in SCADA system // 11th International ISC Conference on Information Security and Cryptology: Proceedings of the International Conference. Iran, Tehran, 3-4 Sept. 2014. Tehran, 2014. P. 55-60.
5. Kim H., Hou J.C. Network calculus based simulation for TCP congestion control: theorems, implementation and evaluation // Proceedings of the Twenty-third Annual Joint Conf. of the IEEE Computer and Communications Societies INFOCOM 2004. 7-11 March 2004. Vol. 4. P. 2844-2855.
6. Масолкин С.И., Промыслов В.Г. Расчет некоторых параметров промышленной вычислительной сети объектов повышенного риска эксплуатации на примере АСУТП АЭС // Проблемы управления. 2010. № 1. С. 47-52.
7. Boyer M., Migge J, Fumey M. PEGASE, a robust and efficient tool for worst case network traversal time // SAE 2011 AeroTech Congress & Exhibition, 2011. 15 p.
8. Байбулатов А.А. От теории очередей к сетевому исчислению: исторический обзор // Труды 11-й Международной конференции «Управление развитием крупномасштабных систем» MLSD'2018. Москва, 1-3 октября 2018 г. М.: ИПУ РАН, 2018. Т. 2. С. 411-421.
9. Le Boudec J.-Y., Thiran P. Network Calculus: A Theory of Deterministic Queuing Systems for the Internet. Online Version of the Book Springer Verlag, LNCS 2050, 2012. 263 p.
10. Poletykin A.G., Promyslov V.G. Digitally Controlled Assets Subjected to Cyberattacks: Definitions and “Cyberproof” Criteria Based on the Analysis of Explicit and Hidden Functions // IFAC Proceedings Volumes. 2013. Vol. 46, No. 9. P. 1038-1042.