Паттерны проектирования архитектуры нулевого доверия

С.С. Валеев, Н.В. Кондратьева

Уфимский университет науки и технологий, г. Уфа

Аннотация: Рассматриваются особенности проектировании систем безопасности на основе модели нулевого доверия и задача разработки паттернов политики безопасности. Обсуждается задача выбора точек применения политики безопасности на основе анализа потока рисков. Приводится пример паттерна безопасности на языке DRAKON.
Ключевые слова: защита информации, архитектура нулевого доверия, архитектура предприятия, паттерны политик безопасности.

Введение

При проектировании информационных систем предприятия (ИСП) в рамках концепции нулевого доверия (НД), возникает задача построения адаптивной системы информационной безопасности [1, 2]. Это связано с необходимостью обеспечения требуемого уровня защищенности ИСП с учетом влияния различных внутренних и внешних факторов неопределенности.

Как известно, архитектура современного предприятия включает в себя бизнес-архитектуру и архитектуру ИСП, которые тесно связаны между собой [3]. Задача внедрения архитектуры НД в ИСП – это минимизация различных рисков для предприятия от возможных атак на информационные активы предприятия, что, в свою очередь, в значительной мере позволяет обеспечить достижение цели предприятия в условиях конкурентной борьбы [4 – 6].

В рамках модели НД основное внимание уделяется использованию обратной связи, необходимой для адаптации политик безопасности в точках их применения [7]. При проектировании систем безопасности в рамках концепции архитектуры НД большое внимание уделяется проектированию точки выбора политики безопасности (ТВПБ) и множества точек применения политики безопасности (ТППБ).

Аудит в реальном времени информационной безопасности ИСП является сложной задачей, как с точки зрения собственно алгоритмической,

так и с точки зрения реализации этих алгоритмов [8]. В настоящее время, для решения этой задачи используются различные подходы, основанные на технологиях больших данных, глубокого обучения, многоагентного подхода и т.д. [9]

Для описания бизнес-процессов используется язык BPMN, при разработке программного обеспечения широко используется язык UML. Одним из языков, используемых на этапе проектирования политики безопасности, является язык DRAKON [10]. Язык DRAKON позволяет также описывать автоматные модели, бизнес-процессы и алгоритмы, задействованные при реализации программного обеспечения.

Паттерны и эталонная архитектура

В общем случае, рассматриваемая архитектура НД представляет собой комбинацию хорошо известных концепций безопасности.

Архитектура НД также поддерживает модель непрерывной безопасности, в которой система безопасности постоянно обучается на входных данных наблюдения (журналы, мониторинг и трассировка) на всех уровнях, получаемых из нескольких облачных ресурсов. Аналитика этого огромного объема данных часто поддерживается моделями машинного обучения, которые позволяют системе динамически формировать набор политик безопасности.

Паттерн проектирования – это формализованное решение повторяющейся программной или системной задачи в рамках архитектурного подхода. В нашем случае, паттерны безопасности описывают, как минимизировать, например, риски нарушения периметра информационной безопасности на основе применяемой политики безопасности в ТППБ.

Рассмотрим далее предлагаемую архитектуру защищенного предприятия (рис. 1).

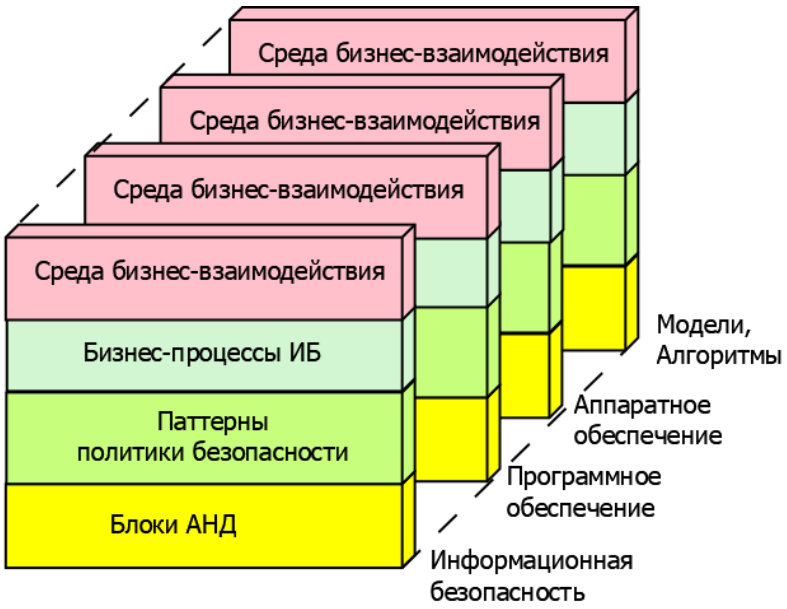

Рис. 1. – Архитектура защищенного предприятия

Архитектура предприятия, в нашем случае, включает несколько горизонтальных слоев: слой информационной безопасности, слой программного обеспечения, слой аппаратного обеспечения и слой моделей, алгоритмов. В свою очередь, все слои включают в себя вертикальные слои: слой блоков, слой паттернов, слой бизнес-процессов и слой среды бизнес-взаимодействия. Данная архитектура предприятия базируется на архитектуре Гартнера [3]. Особенностью этой архитектуры является ее простота и охват архитектурных основных элементов современного предприятия.

Отличительной особенностью рассматриваемой архитектуры предприятия является включение горизонтального слоя информационной безопасности. Этот слой включает блоки архитектуры нулевого доверия: ТВПБ, ТППБ, основные элементы политик безопасности.

Паттерны политики безопасности включают абстрактное описание на языке DRAKON шаблонов доступа для различных версий политик безопасности (см. рис. 2).

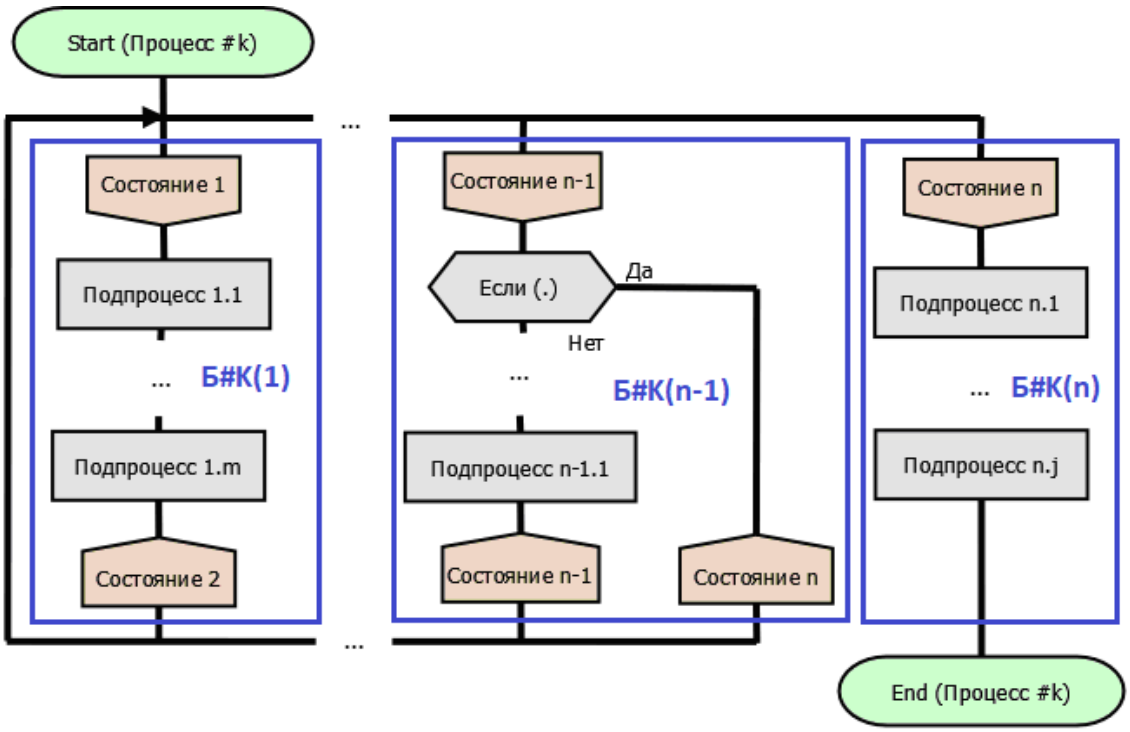

Рис. 2. – Паттерн политики безопасности на языке DRAKON, где k – процесса, Б#k(i) – i-й блок архитектуры НД.

На рис. 3 представлена модель максимального потока рисков в ИСП в виде графа G= (V, P), где V – множество вершин графа (точки применения политики безопасности, активы), P – множество ребер графа (качественно отражающие вероятности распространения рисков в системе). Значения весов $p_{i,j}$ определяются группой экспертов и являются оценками эффективности средств обеспечения информационной безопасности.

Как следует из анализа графа G пути от вершины v_0 (субъект) через вершины v_1,v_4 к вершине v_8 (актив) и через вершины v_2,v_8 имеют высокую пропускную способность для распространения рисков. Тем самым, при проектировании архитектуры НД, следует в этих вершинах разместить точки применения политики безопасности, например, используя обобщенный шаблон, представленный на рисунке 2.

На рис. 4 представлена возможная реализация политики безопасности “Вход в систему” (паттерн), описанная на языке DRAKON.

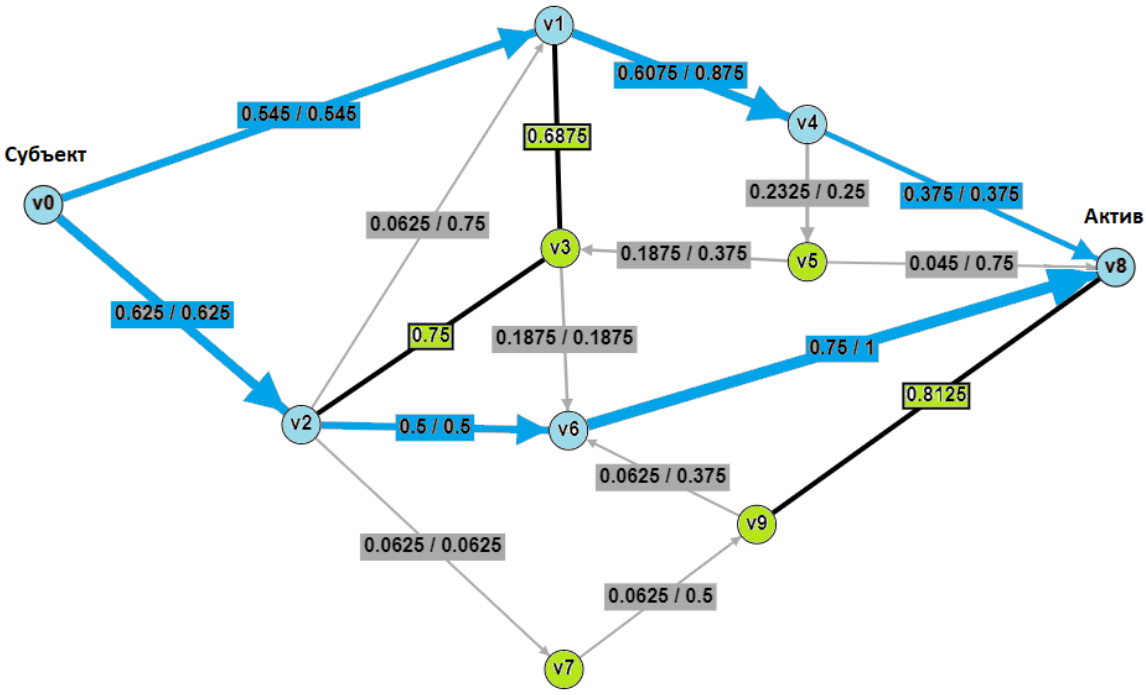

Рис. 3. – Модель определения максимального потока рисков в ИСП

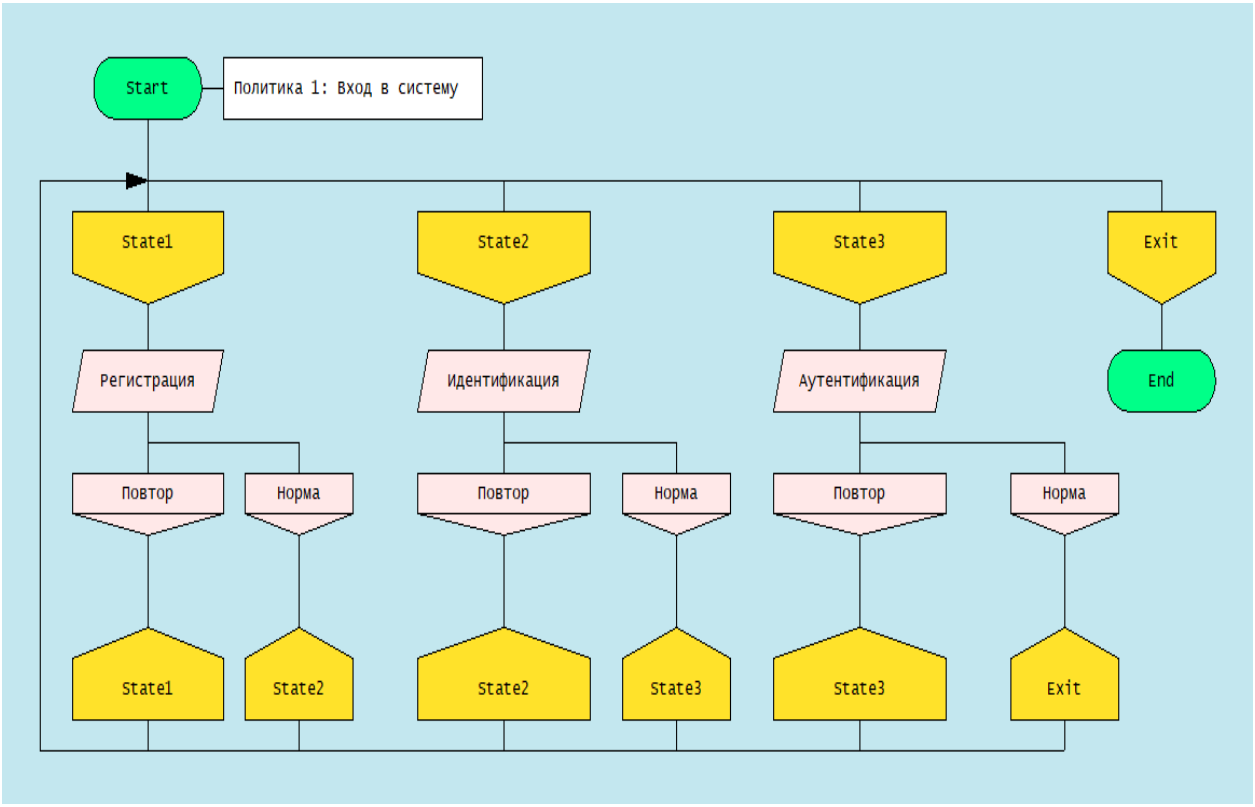

Рис. 4. – Паттерн политики безопасности “Вход в систему”

Данный паттерн содержит блоки архитектуры НД: “регистрация”, “идентификация” и “аутентификации”. В зависимости от того, какой субъект запрашивает доступ к информационному активу предприятия, система ТВПБ определяет наполнение ТППБ (формирует содержимое блоков, используемого паттерна безопасности).

Заключение

При проектировании систем информационной безопасности предприятия на основе архитектуры нулевого доверия необходим сбор большого объема данных. Эти данные позволяют решить задачу обучения классификатора для формирования текущей политики безопасности. Обсуждается формирование паттернов политики безопасности на основе языка DRAKON. Рассматривается пример паттерна политики безопасности. Представлена разработанная модель максимального потока рисков, используемая для выбора точек применения политики безопасности. Предложенный подход позволит повысить эффективность процесса проектирования ИСП на предпроектном этапе жизненного цикла системы.

Литература

1. He Y., Huang D., Chen L., Ni Y., Ma X. A Survey on Zero Trust Architecture: Challenges and Future Trends // Wirel. Commun. Mob. Comput. 2022, №6476274 URL: hindawi.com/journals/wcmc/2022/6476274/.

2. Валеев С.С., Кондратьева Н.В. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия // Инженерный вестник Дона. 2023. №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8627.

3. Ендовицкий Д.А. Архитектура предприятия. М.: КНОРУС, 2021. 352 с.

4. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона. 2022. № 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

5. Макарова Л.В., Филонова Ю.Б. Комплексный подход к оценке конкурентоспособности предприятия // Инженерный вестник Дона, 2023, №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8598.

6. Акупиян О.С., Коршунов А.Г., Ломазов В.А., Кравченко Д.П. Выбор стратегий обеспечения информационной безопасности объекта защиты в условиях неопределенности и противодействия // Инженерный вестник Дона, 2023, №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8621.

7. Валеев С.С., Кондратьева Н.В., Мельников А.В. Архитектура предприятия и архитектура нулевого доверия // Вестник УрФО. Безопасность в информационной сфере, 2023, Т. 2, № 48. С. 49–53.

8. Валеев С.С., Кондратьева Н.В. Анализ бизнес-процессов в распределенной организационно-технической системе на основе снимков состояния // Вычислительные технологии, 2023, Т. 28, № 1. С. 41–47.

9. Mandal D., Singhal N., Tyagi M. Cybersecurity in the Era of Emerging Technology // Emerging Technology and Management Trends. 2023, № 1. pp. 108–134.

10. Пароджанов В.Д. Алгоритмизация медицины и реформа медицинского языка // Евразийский Союз Ученых. 2015. №11-1 (20). URL: cyberleninka.ru/article/n/algoritmizatsiya-meditsiny-i-reforma-meditsinskogo-yazyka.

References

1. He Y., Huang D., Chen L., Ni Y., Ma X. A Survey on Zero Trust Architecture: Challenges and Future Trends // Wirel. Commun. Mob. Comput. 2022, №6476274. URL: hindawi.com/journals/wcmc/2022/6476274/.

2. Valeev S.S., Kondratyeva N.V. Inzhenernyj vestnik Dona, 2023, №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8627.

3. Endovickij D.A. Arhitektura predprijatija [Enterprise architecture]. M.: KNORUS, 2021. 352 p.

4. Ibragimova Z.M., Batchaeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, № 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010.

5. Makarova L.V., Filonova Yu. B. Inzhenernyj vestnik Dona, 2023, №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8598.

6. Akupiyan O.S., Korshunov A.G., Lomazov V.A., Kravchenko D.P. Inzhenernyj vestnik Dona, 2023, №8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8621.

7. Valeev S.S., Kondrat'eva N.V., Mel'nikov A.V. Vestnik UrFO. Bezopasnost' v informacionnoj sfere (Rus), 2023, T. 2, № 48. pp. 49-53.

8. Valeev S.S., Kondrat'eva N.V. Vychislitel'nye tehnologii, 2023, V. 28, № 1. pp. 41-47.

9. Mandal D., Singhal N., Tyagi M. / Emerging Technology and Management Trends. 2023, № 1. pp. 108–134.

10. Parondzhanov V.D. Evrazijskij Soyuz Ucheny`x, 2015, №11-1 (20). URL: cyberleninka.ru/article/n/algoritmizatsiya-meditsiny-i-reforma-meditsinskogo-yazyka.