УДК 004.056.5:519.876.5 Вестник УрФО № 2(48) / 2023, с. 49–53

Валеев С.С., Кондратьева Н.В., Мельников А.В. DOI: 10.14529/secur230204

АРХИТЕКТУРА ПРЕДПРИЯТИЯ И АРХИТЕКТУРА НУЛЕВОГО ДОВЕРИЯ

Рассмотрена задача разработки архитектуры предприятия с учетом концепции архитектуры нулевого доверия. Обсуждаются особенности иерархической архитектуры информационной системы управления и возможная организация архитектуры нулевого доступа с применением эталонных моделей бизнес-процессов. Предлагается рассматривать бизнес-процесс предприятия как участника обмена информацией по защищенному протоколу в рамках архитектуры нулевого доверия.

Ключевые слова: *архитектура нулевого доверия, архитектура предприятия, бизнес-процесс, стандарты безопасности, система сбора информации, система управления технологическими процессами.*

Valeev S.S., Kondratyeva N.V., Melnikov A.V.

ENTERPRISE ARCHITECTURE AND ZERO TRUST ARCHITECTURE

The problem of developing enterprise architecture is considered, taking into account the concept of zero trust architecture. The features of the hierarchical architecture of an information management system and the possible organization of a zero-access architecture using reference models of business processes are discussed. It is proposed to consider the business process of an enterprise as a participant in the exchange of information over a secure protocol within the framework of zero trust architecture.

Keywords: *zero trust architecture, enterprise architecture, business process, security standards, data acquisition system, process control system.*

Введение

В архитектуре предприятия отражается как в зеркале вся сложность выполняемых бизнес процессов, в том числе и процессов обеспечения промышленной и информационной безопасности [1-4]. В условиях эволюционного развития промышленных предприятий возникают проблемы, связанные с соответствием систем безопасности новым требованиям и стандартам [5]. При сертификации объектов критической инфраструктуры особое внимание уделяется выполнению критериев обеспечения промышленной безопасности и противодействию угроз, связанных с цифровыми системами сбора информации и системами управления технологическими процессами [6].

Рассмотрим далее развиваемую в настоящее время концепцию защиты информации - архитектуру нулевого доверия и особенности ее использования при проектировании архитектуры предприятия [7].

Архитектура нулевого доверия (АНД) – это интегрированная платформа безопасности, которая использует контекстную информацию из удостоверений, безопасности и ИТ-инфраструктуры, а также инструменты анализа рисков и аналитики для информирова-

ния и обеспечения динамического применения политик безопасности единообразно по всему предприятию. АНД переводит безопасность с неэффективной модели, ориентированной на периметр, на модель, ориентированную на ресурсы и идентификацию. В результате организации могут постоянно адаптировать средства управления доступом к меняющейся среде, повышая безопасность, снижая риски, упрощая и отказоустойчивые операции и повышая гибкость бизнеса.

Требования к архитектуре нулевого доверия

Рассмотрим далее базовый набор требований к платформе АНД [7]. Связь между субъектами обмена данных должна быть зашифрована. Система защиты должна обеспечивать контроль доступа ко всем типам ресурсов. Механизмы управления доступом должны управляться ориентированными на идентичность и контекстуальными политиками. Средства защиты ресурсов данных должны иметь возможность использовать идентификационные и контекстные политики для управления доступом. Что касается модели, то модель системы и политики безопасности должна поддерживать безопасность всех пользователей во всех местах, а модель политики и элементов управления должны быть согласованы для удаленных и локальных пользователей. При этом все устройства должны иметь возможность проверять состояние безопасности и конфигурацию до предоставления доступа и периодически после этого. Доступ к любому сетевому ресурсу должен быть явно разрешен политикой, т.е. ни один пользователь или устройство не должны иметь широкий доступ к сети.

Элементы управления доступом должны иметь возможность различать разные службы на одном и том же сетевом ресурсе. Например, доступ к HTTPS должен предоставляться отдельно от доступа к SSH. В то же время, доступ к определенным элементам данных, содержащимся в приложениях или контейнерах, которые имеют разные классификации, должен обеспечиваться на основе соответствующих административных мер.

Метаданные сетевого трафика должны регистрироваться и дополняться контекстом идентификации. Более того, должна быть предусмотрена возможность проверки сетевого трафика в целях безопасности и предотвращения потери данных. При этом рабочие нагрузки, переносимые в облако, должны включать те же политики управления доступом, что и локальные решения.

Автоматизация должна включать детали, ориентированные на идентификацию, чтобы обеспечить эффективное и действенное реагирование на инциденты.

Журналы должны быть включены в инструменты аналитики для эффективного и динамичного применения политик.

Архитектура предприятия и архитектура нулевого доверия

Рассмотрим далее обобщенную архитектуру современного предприятия (рис. 1), включающую иерархическую систему управления данным предприятием и иерархию базовых бизнес-процессов. Представленная архитектура базовых бизнес-процессов отражает обобщенную иерархическую структурную организацию предприятия и включает в себя защищенную коллекцию основных бизнес-процессов, обеспечивающих заданную эффективность жизненного цикла производственного процесса [8].

В качестве основных элементов коллекции выбираются верифицированные бизнес-процессы, модели которых разработаны для различных уровней системы управления предприятием, а также, реализованы защищенные интерфейсы обмена информацией между различными уровнями управления и соответствующими базами данных [9].

В базе данных моделей хранятся журналы исполненных бизнес-процессов и оценка их эффективности (БД_МЦ), журналы исполненных бизнес-процессов уровня координации (БД_МК) и информация об актуальном состоянии бизнес-процессов предприятия в текущий момент времени (БД_МЗ).

На основе данных из этих источников можно восстановить пространство состояний актуальных бизнес-процессов, решать задачи оценки состояния производства, прогнозировать характеристики этапов жизненного цикла процессов и, в случае необходимости, выбрать требуемое управленческое решение [10, 11].

Для внедрения АНД в архитектуру предприятия необходимо сформировать множество субъектов S доступа к информационным активам предприятия I и сформировать множество бизнес-процессов B. Разработать политики аутентификации P, реализовать защищенный обмен информацией T. Данные процедуры необходимо выполнить для всех иерархических уровней архитектуры (рис. 1).

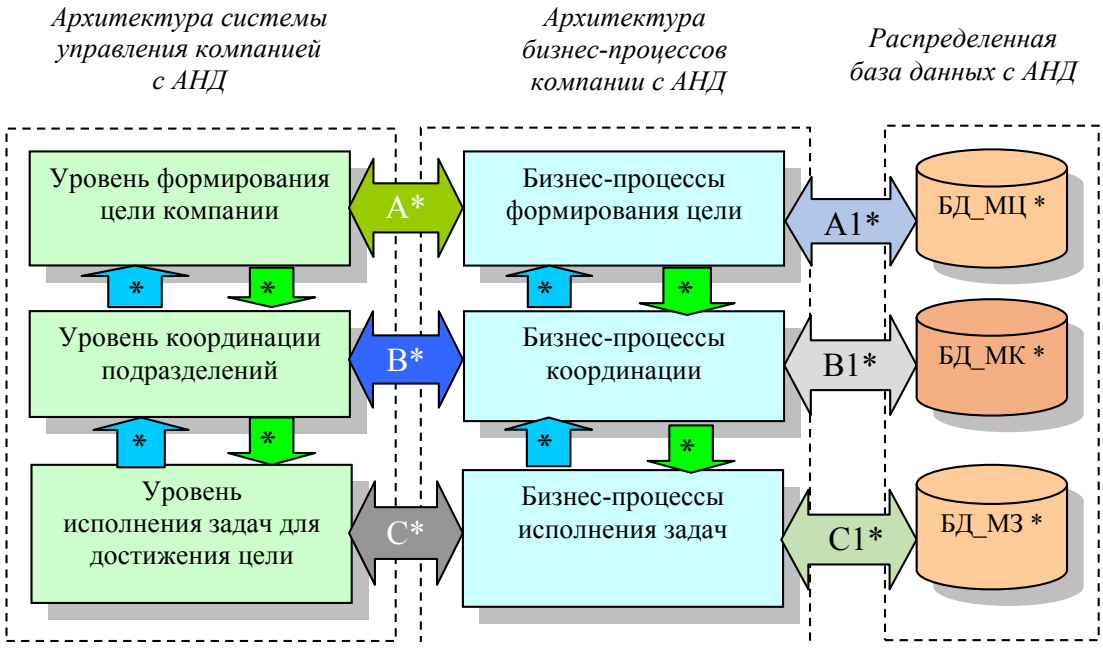

Рис. 1. Иерархическая архитектура предприятия, где * – различные элементы реализации АНД

Тогда иерархическую АНД можно представить следующим образом:

$$Z_i = (S_i, I_i, B_i, P_iT_i),\ i = 1..3.$$

Следует заметить, что с учетом сложности защищаемых объектов, сложность реализации алгоритмов защиты информации связана с комбинаторной сложностью.

Эталонные модели бизнес-процессов как элементы архитектуры предприятия

Для решения задачи аутентификации бизнес-процессов в рамках АНД необходима разработка коллекции эталонных моделей для выполняемых на предприятии бизнес-процессов.

При разработке этих моделей используются различные языки моделирования сложных процессов, например, UML 2.0, BPMN и язык DRAKON. В результате работы аналитиков предприятия, создается база эталонных моделей (ЭМ), которая является одним из основных активов промышленного предприятия.

С помощью этих ЭМ бизнес-процессов, построенных для различных уровней иерархической системы управления, оцениваются ключевые показатели эффективности исполнения этих процессов, что позволяет, в свою очередь, выявить слабые звенья в последовательности исполняемых бизнес-процессов.

Как показывает практика, на сегодняшний день не разработаны обобщенные эталонные модели для паттернов бизнес-процессов, которые можно было бы использовать для автоматизации процессов управления предприятием [9]. Процедура разработки ЭМ бизнес-процессов в нашем случае включает следующие основные этапы: построение формализованных моделей бизнес-процессов, внедрение их в архитектуру предприятия в качестве элементов и интеграцию их защищенного взаимодействия рамках концепции АНД.

Следует отметить, что для решения этой задачи необходима обработка больших массивов неструктурированных и разнородных данных. Тем самым, возникает задача привлечения технологий обработки нарастающих данных, что в свою очередь, также требует необходимости учета этого в политике безопасности предприятия.

На рис. 2 представлена обобщенная архитектура информационной системы промышленного предприятия с элементами АНД, где – ЗКС- защищенный канал связи, ДМЗ – демилитаризованная зона, ТППБ – точка применения политики безопасности, БД – базы данных, БП – бизнес-процесс.

Точка применения политики безопасности (ТППБ) отвечает за получение запросов на авторизацию, которые отправляются в точку принятия решения о политике для оценки. ТППБ может находиться в любом месте приложения, где данные и ресурсы должны быть защищены или где применяется логика авторизации.

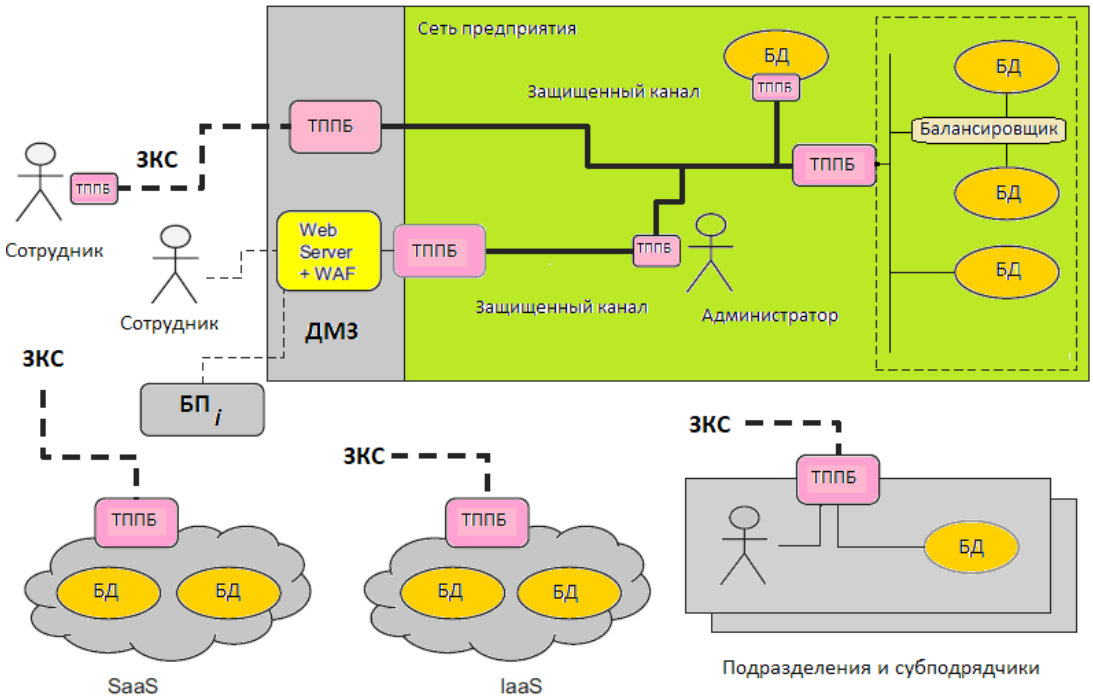

Рис. 2. Обобщенная архитектура информационной системы промышленного предприятия с элементами АНД

Заключение

Рассмотрена задача разработки архитектуры предприятия с учетом концепции архитектуры нулевого доверия. Предлагается рассматривать бизнес-процесс предприятия как равноправного участника обмена информацией по защищенному протоколу в рамках архитектуры нулевого доверия. Отмечается, что сложности достижения целей архитектуры нулевого доверия потребует значительного увеличения вычислительных ресурсов. Обсуждаются особенности иерархической архитектуры информационной системы управления и возможная организация архитектуры нулевого доступа с применением эталонных моделей бизнес-процессов.

Литература

1. Аббазов В.Р., Балуев В.А., Мельников А.В., Русанов М.А. Метод нахождения связанных показателей на основе анализа нормативно-правовых актов методами NLP // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2022. Т. 22. № 1. С. 88–96.

2. Стасинопулос П. Проектирование систем как единого целого. – М.: Эксмо, 2012. – 288 с.

3. Valeev S., Kondratyeva N., Process Safety and Big Data, Elsevier, Amsterdam, Netherlands, 2021, DOI: https://doi.org/10.1016/C2019-0-03546-7.

4. Rusanov M.A., Abbazov V.R., Baluev V.A., Burlutsky V.V., Melnikov A.V. On the approach to forecasting indicators of socio-economic development of the region based on indirect indicators Modeling, Optimization and Information Technology. 2022. V. 10. № 3 (38). С. 2–3.

5. Литвинов Г.А., Щерба Е.В. Применение моделей доверия и репутации для обеспечения безопасности маршрутизации в динамически организуемых сетях // Вестник УрФО. Серия: Безопасность в информационной сфере. 2021. № 3(41). С. 12–23.

6. Басыня Е. А., Сафронов А. В. Децентрализованный подход к сбору и обработке данных информационной инфраструктуры предприятия // Вестник УрФО. Серия: Безопасность в информационной сфере. 2019. № 3(33). С. 43–54.

7. Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], DOI: https://doi.org/10.6028/NIST.SP.800-207.

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

9. 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.

10. Ларман К. Примнение UML 2.0 и шаблонов проектирования. – М.: Диалектика, 2020. – 736 с.

11. Косяков А., Свит У. и др. Системная инженерия. – М.: ДМК Пресс, 2014. – 624 с.

References

1. Abbazov V.R., Baluyev V.A., Mel'nikov A.V., Rusanov M.A. Metod nakhozhdeniya svyazannykh pokazateley na osnove analiza normativno-pravovykh aktov metodami NLP // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternyye tekhnologii, upravleniye, radioelektronika. 2022. T. 22. № 1. S. 88–96.

2. Stasinopulos P. Proyektirovaniye sistem kak yedinogo tselogo. – M.: Eksmo, 2012. – 288 s.

3. Valeev S., Kondratyeva N., Process Safety and Big Data, Elsevier, Amsterdam, Netherlands, 2021, DOI: https://doi.org/10.1016/C2019-0-03546-7.

4. Rusanov M.A., Abbazov V.R., Baluev V.A., Burlutsky V.V., Melnikov A.V. On the approach to forecasting indicators of socio-economic development of the region based on indirect indicators. Modeling, Optimization and Information Technology. 2022. V. 10. № 3 (38). C. 2–3.

5. Abbazov V.R., Baluyev V.A., Mel'nikov A.V., Rusanov M.A. Metod nakhozhdeniya svyazannykh pokazateley na osnove analiza normativno-pravovykh aktov metodami NLP // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Komp'yuternyye tekhnologii, upravleniye, radioelektronika. 2022. T. 22. № 1. S. 88–96.

6. Stasinopulos P. Proyektirovaniye sistem kak yedinogo tselogo. – M.: Eksmo, 2012. – 288 s

7. Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], DOI: https://doi.org/10.6028/NIST.SP.800-207.

8. Yendovitskiy D.A. Arkhitektura predpriyatiya. – M.: KNORUC, 2021. – 352 s.

9. Valeyev S.S., Kondrat'yeva N.V. Analiz biznes-protsessov v raspredelennoy organizatsionno-tekhnicheskoy sisteme na osnove snimkov sostoyaniya // Vychislitel'nyye tekhnologii. 2023. T. 28. № 1. S. 41–47.

10. Larman K. Primneniye UML 2.0 i shablonov proyektirovaniya. – M.: Dialektika, 2020. – 736 c.

11. Kosyakov A., Svit U. i dr. Sistemnaya inzheneriya. – M.: DMK Press, 2014. – 624 s.

ВАЛЕЕВ Сагит Сабитович, доктор технических наук, профессор, Сочинский государственный университет. Россия, 354008, г. Сочи, ул. Пластунская, 94. E-mail: vss2000@mail.ru

КОНДРАТЬЕВА Наталья Владимировна, кандидат технических наук, доцент, Сочинский государственный университет. Россия, 354008, г. Сочи, ул. Пластунская, 94. E-mail: knv24@mail.ru

МЕЛЬНИКОВ Андрей Витальевич, доктор технических наук, профессор, Автономное учреждение Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информационных технологий». Россия, 628011, г. Ханты-Мансийск, ул. Мира, 151. E-mail: MelnikovAV@uriit.ru

VALEEV Sagit Sabitovich, Doctor of Technical Sciences, Professor, Sochi State University. Russia, 354008, Sochi, Plastunskaya Str., 94. E-mail: vss2000@mail.ru

KONDRATYEVA Natalya Vladimirovna, Candidate of Technical Sciences, Associated Professor, Sochi State University. Russia, 354008, Sochi, Plastunskaya Str., 94. E-mail: knv24@mail.ru

MELNIKOV Andrey Vitalyevich, Doctor of Technical Sciences, Professor, Autonomous institution of the Khanty-Mansiysk Autonomous Okrug - Yugra "Ugra Research Institute of Information Technologies". Russia, 628011, Khanty-Mansiysk, Mira Str., 151. E-mail: MelnikovAV@uriit.ru