Инженерный вестник Дона, №8 (2023)
ivdon.ru/ru/magazine/archive/n8y2023/8627

Особенности проектирования систем безопасности на базе архитектуры нулевого доверия

С.С. Валеев, Н.В. Кондратьева

Уфимский университет науки и технологий, г. Уфа

Аннотация: Для оптимизации жизненного цикла информационных систем при проектировании используются абстрактные модели, описывающие основные элементы архитектуры системы. Архитектура нулевого доверия – новая концепция информационной безопасности, учитывающая удаленный формат доступа сотрудников к активам информационной системы предприятия. Рассматриваются основные особенности архитектуры нулевого доверия.
Ключевые слова: защита информации, информационная система предприятия, архитектура нулевого доверия, политика безопасности.

Введение

Информационные системы предприятия (ИСП) решают важную задачу обеспечения защищенного доступа к активам предприятия и удаленных офисов. От эффективности решения этой задачи зависит не только выполнение бизнес-процессов в условиях влияния деструктивных факторов, но и само существование современного предприятия [1, 2]. Корпоративные ИСП можно отнести к классу сложных организационно-технических систем, включающих аппаратно-программные комплексы, персонал, а также системы энергоснабжения.

Задача проектирования ИСП относится к классу сложных инженерных задач. Это связано с длительным жизненным циклом развития предприятия, адаптацией целей предприятия с учетом влияния различных факторов неопределенности, что отражается и на процессах развития ИСП [3]. Концепция поддержки жизненного цикла сложной производственной системы и ее ИСП основана на использовании абстрактных моделей, или архитектуры предприятия. На Рисунке 1 представлены основные элементы архитектуры предприятия [4, 5]. Архитектура предприятия включает в себя бизнес-архитектуру и архитектуру информационной системы тесно связанных между собой.

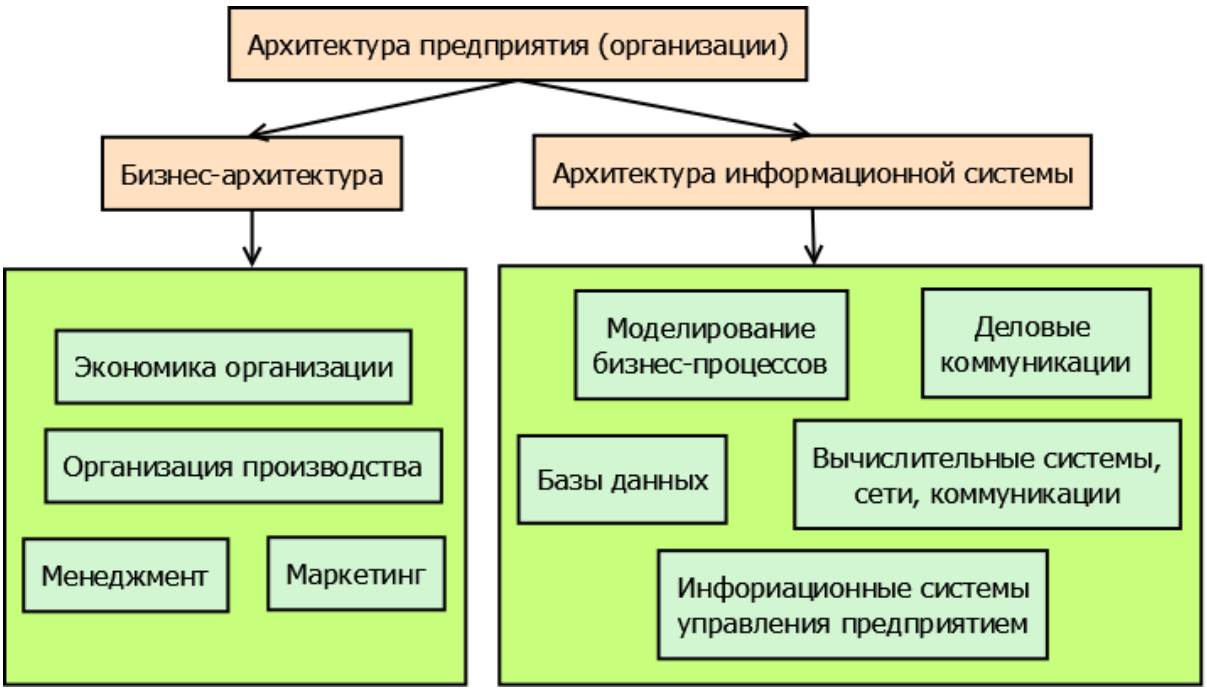

Рис. 1. – Архитектура предприятия

Использование удаленного доступа сотрудниками предприятия изменило процедуры доступа к активам ИСП и привело к необходимости сотрудникам, работающих в удаленном режиме, обеспечить доступ со своих компьютеров или телефонов к различным информационным сервисам и корпоративным базам данных. Это изменило границы ИСП – они стали размытыми [6].

Следует отметить, что распределенные и фрагментированные ИСП более уязвимы с точки зрения обеспечения информационной безопасности. Интеграция офисных и домашних информационных систем объединяет системы с различными моделями безопасности, это затрудняет управление безопасностью распределенной интегрированной ИСП в рамках разработанной и утвержденной на предприятии политики безопасности (ПБ).

Как известно, ПБ предприятия включает совокупность правил, процедур или руководящих принципов в области безопасности для предприятия.

Концепция архитектуры нулевого доверия

Архитектура нулевого доверия (АНД) – новая концепция в области информационной безопасности (ИБ), отражающая тенденции развития ИСП и архитектуры систем информационной безопасности (ИБ) [7–9]. Основная задача АНД – минимизация рисков ИБ на предприятии от последствий возможных атак на информационные активы предприятия, что, в свою очередь, обеспечивает эффективное решение задач предприятия [10].

АНД – это *набор руководящих принципов* для организации процессов ИБ, проектирования системы безопасности, которые можно использовать для повышения уровня безопасности ИСП.

В модели безопасности с нулевым доверием (НД) предполагается, что злоумышленник, находящийся во внешней среде, может присутствовать и в среде, принадлежащей предприятию, и они ничем не отличаются. Тем самым, в рамках этой модели предприятие должно отказаться от безоговорочного доверия к своим сотрудникам и постоянно анализировать, оценивать риски ИБ для своих активов, риски нарушения бизнес-процессов. Предполагается, что необходимо постоянно принимать меры информационной защиты для снижения этих рисков.

В рамках этой концепции предполагается, что при допуске к активам или учетным записям пользователей осуществляется постоянная проверка их местоположения, идентификатор устройства, тип операционной системы, особенности использования активов. Таким образом, в ПБ доступа к активам предприятия может учитываться большее количество информации о субъекте и ПБ может изменяться по заданным правилам адаптивной системой безопасности.

На Рисунке 2 представлена обобщенная архитектура системы ИБ на основе модели НД. Она состоит из двух основных уровней: уровня доступа субъекта к активам предприятия и уровня предприятия с его активами.

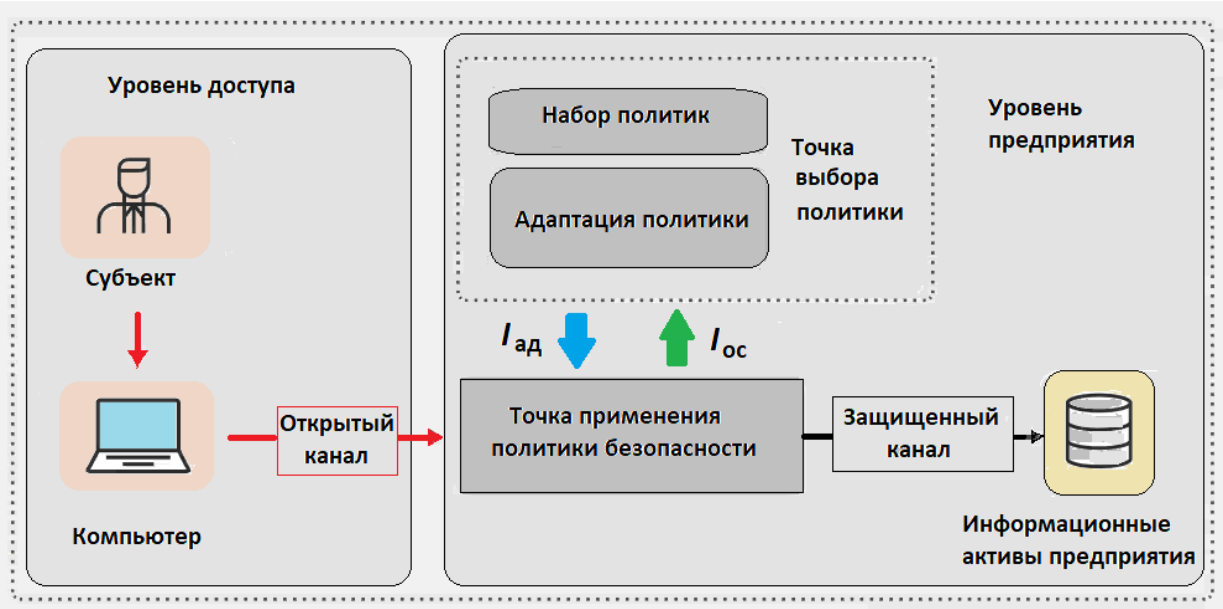

Рис. 2. – Доступ субъекта к активам предприятия на основе модели нулевого доверия

Субъект формирует запрос на разрешение входа в ИСП и отправляет его по открытому каналу. Запрос поступает на точку применения политики безопасности (ТППБ). Политика безопасности формируется и выбирается точкой выбора политики (ТВПБ) и передается в ТППБ.

Вся доступная информация, получаемая об активности субъекта $I_{ОС}$ передается в блок выбора политики безопасности, где после анализа в случае необходимости она может корректироваться блоком адаптации политик ТВПБ и передаваться в виде скорректированной политики безопасности $I_{АД}$ в ТППБ. После получения разрешения субъект по защищенному каналу получает доступ к активам предприятия.

Особенности проектирования архитектуры нулевого доверия

По результатам проведенного анализа можно выделить следующие особенности проектирования систем ИБ на основе АНД.

В ИСП обрабатываются все больше и больше различной информации, что отражает сложность бизнес-процессов предприятия. При этом используются различные внутренние компьютерные сети, связанные с

удаленными подразделениями, которые, в свою очередь, имеют свои ИС. Методы обеспечения сетевой ИБ, основанные на концепции периметра безопасности в современных условиях не могут обеспечить требуемый уровень информационной безопасности, поскольку для распределенного предприятия нет единого, четко идентифицируемого периметра информационной безопасности. Таким образом, если злоумышленники смогли преодолеть периметр безопасности, то дальнейшее горизонтальное перемещение в сети для них становится беспрепятственным. В этом случае применение АНД оправдано.

Модель АНД в первую очередь ориентирована на защиту данных и услуг, но может быть расширена на все активы предприятия (устройства, компоненты инфраструктуры, приложения, виртуальные и облачные компоненты), а также субъектов (конечных пользователей, приложений и других информационных объектов, которые запрашивают информацию). При этом доступ разрешен только тем субъектам и активам, которые определены как *нуждающиеся* в доступе, а также если при этом обеспечивается выполнение *постоянной аутентификации* и *авторизации* личности и *анализ состояния* безопасности каждого запроса на доступ в систему.

При проектировании систем безопасности в рамках концепции АНД большое внимание необходимо уделять проектированию ТВПБ и оптимальному выбору множества ТППБ.

Формирование политик безопасности P_i для каждого i-го субъекта требует обработки большого массива данных D_i, хранящихся в журналах, в которых регистрируется действия всех субъектов. На основе этих данных с помощью алгоритмов классификации принимается решение об изменении правил ПБ и выполняется адаптация политики P_i для i-го субъекта.

При проектировании программных систем в настоящее время используются различные паттерны (шаблоны) проектирования (ПП), в

которых отражается накопленный опыт разработчиков ИСП. Учитывая, что при переходе на новую архитектуру часто в качестве основы используется существующая ИСП, то накопленный опыт применения ПП может сократить время перехода и повысить эффективность применяемых решений.

Для реализации процедуры динамического формирования множества политик безопасности требуется сбор и анализ нарастающих данных, дополнительные затраты на организацию и сопровождение хранения, обработки массивов информации, используемой для решения задачи адаптации политик безопасности контроля доступа субъектов к активам предприятия.

Заключение

В настоящее время сотрудники предприятия могут работать дистанционно и имеют доступ к активам предприятия. Традиционная модель обеспечения информационной безопасности, основанная на периметре безопасности, не позволяет обеспечить требуемый уровень защиты от возможных угроз. Архитектура нулевого доверия направлена на решение данной проблемы и позволяет обеспечить постоянный контроль доступа к активам предприятия. Основным элементом этой архитектуры является динамически изменяемая персонифицированная политика безопасности для субъектов.

Как показывает анализ особенностей АНД, при проектировании системы безопасности на этапе разработке требований к системы безопасности ИСП необходимо задать множество ТППБ и определить в рамках ПБ предприятия множество политик безопасности для субъектов доступа к активам предприятия. При решении данной задачи приходится учитывать множество различных факторов: ценность активов, прав доступа к ним и т.п., что значительно усложняет процедуру проектирования и реализации АНД.

Литература

1. 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.

2. 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.

3. 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.

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

5. Valeev S., Kondratyeva N. Process Safety and Big Data. Amsterdam: Elsevier, 2021. 312 p. URL: sciencedirect.com/book/9780128220665/ process-safety-and-big-data.

6. Федченко А.А. Удаленная работа в условиях использования цифровых технологий: перспективы трансформации // Экономика труда, 2021, том 8, № 4. С. 377–390 URL: 1economic.ru/lib/111930.

7. Rose S., et al. Zero Trust Architecture, Special Publication (NIST SP). Gaithersburg: National Institute of Standards and Technology, 2020. URL: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

8. 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/

9. 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.

10. Хромова А.Р., Петросян Л.Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона, 2023, №6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8447.

References

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

2. Valeev S.S., Kondrat'eva N.V. Vychislitel'nye tehnologii, 2023, T. 28, № 1. pp. 41-47.

3. 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.

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

5. Valeev S., Kondratyeva N. Process Safety and Big Data. Amsterdam: Elsevier, 2021. 312 p. URL: sciencedirect.com/book/9780128220665/process-safety-and-big-data.

6. Fedchenko A.A. E`konomika truda, 2021, tom 8, № 4. pp. 377–390 URL: 1economic.ru/lib/111930.

7. Rose S., et al. Zero Trust Architecture, Special Publication (NIST SP). Gaithersburg: National Institute of Standards and Technology, 2020. URL: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

8. He Y., Huang D., Chen L., Ni Y., Ma X. Wirel. Commun. Mob. Comput. 2022, №6476274 URL: hindawi.com/journals/wcmc/2022/6476274/

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

10. Xromova A.R., Petrosyan L.E`. Inzhenernyj vestnik Dona, 2023, №6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8447.