Инженерный вестник Дона, №5 (2025)
ivdon.ru/ru/magazine/archive/n5y2025/10046

Особенности реагирования на инциденты в пространственно-распределенных автоматизированных информационных системах

А.В. Кузнецов

Финансовый университет при Правительстве Российской Федерации

Аннотация: В статье представлены результаты анализа особенностей построения и сопровождения современных пространственно-распределенных автоматизированных информационных систем, включая модели организации работ команд сопровождения, а также особенности реагирования на возникающие в них инциденты информационной безопасности. Предложены факторы, которые должны быть учтены при планировании и реализации мер реагирования на инциденты информационной безопасности: используемая модель организации работы группы реагирования; используемое количество независимых каналов связи; целевое временя восстановления системы; целевая точка восстановления системы; ограничения области реагирования на инциденты информационной безопасности (локализации) в автоматическом режиме. Полученные результаты позволяют повысить эффективность проводимых мероприятий по планированию и реализации мер реагирования на инциденты информационной безопасности, возникающие в рамках пространственно-распределенных автоматизированных информационных систем.
Ключевые слова: мера реагирования, группа реагирования, кибератака, компьютерная сеть, канал связи

Введение

Распределенные в пространстве (по территории) автоматизированные информационные системы (РАИС) стали неотъемлемой частью деятельности современных ведомств, организаций и предприятий [1]. Они используются в различных сферах, включая медицину, энергетику, финансы, связь и государственное управление. С одной стороны, РАИС позволяют эффективно обрабатывать большие объемы данных и обеспечивать высокую доступность данных и сервисов для потребителей (в ряде случаев РАИС представляют собой кластеры пространственно-сосредоточенных автоматизированных информационных систем [2]). Но, с другой стороны, их распределенная природа делает РАИС уязвимыми для компьютерных атак (кибератак), в т. ч. в менее подготовленных местах, приводящих к различным инцидентам информационной безопасности (ИБ), число которых непрерывно растет [3]. Таким образом, обеспечение ИБ РАИС, в т. ч. организация и

реализация мер реагирования на инциденты ИБ, является актуальной научно-практической задачей.

Цель, задачи, материалы и методы исследования

Целью настоящего исследования является повышение эффективности проводимых мероприятий по планированию и реализации мер реагирования на инциденты ИБ, возникающие в рамках РАИС.

Для достижения поставленной цели предлагается:

1) Проанализировать особенности построения и сопровождения РАИС.

2) Определить факторы, которые должны быть учтены при реагировании на инциденты ИБ.

Автором проводился анализ и синтез на базе общедоступных отчетов, научно-исследовательский статей и монографий.

За рамками настоящего исследования: РАИС специального и военного назначения.

Особенности построения и сопровождения РАИС

К примерам РАИС, услуги которых прямо или косвенно могут потреблять большинство граждан, можно отнести следующие системы:

- Единая государственная информационная система в области здравоохранения (ЕГИСЗ) [4], аналогичные системы представлены и в других странах (например: Electronic Health Records в США, Electronic Medical Record в Китае, Canada Health Infoway и Канаде);

- системы управления энергосетями (Smart Grid) [5], представленные во всех развитых странах [6];

- Единая биометрическая система (ЕБС) [7], около сотни стран уже используют программы электронных паспортов с биометрией [8].

Перечисленные примеры наглядно демонстрируют, что РАИС используются для решения масштабных задач, играют ключевую роль в

управлении государственными ресурсами и предоставлении услуг гражданам. В России большая часть РАИС является государственными информационными системами (ГИС), при определении класса защищенности которых учитывается их масштаб: федеральный или региональный в контексте данного исследования.

Кибератаки на РАИС достаточно актуальны, особенно в складывающихся условиях геополитического противоборства. К наиболее ярким примерам кибератак можно отнести:

- кибератаку на Colonial Pipeline (2021 г., США), управляющей трубопроводом для перекачки топлива на восточном побережье США (время простоя: пять дней; выкуп $4,4 млн в биткоинах);

- кибератаку на систему здравоохранения (2017 г., Великобритания), обеспечивающую Национальную службу здравоохранения Великобритании (время простоя: несколько дней в некоторых больницах);

- кибератаки на систему управления энергосетями (2015 г., Украина), обеспечивающую управление электрическими подстанциями (время простоя: от нескольких часов до нескольких дней в зависимости от региона).

РАИС состоят из множества узлов (в т. ч. кластеров узлов), которые географически (территориально) распределены и взаимодействуют через различные компьютерные сети, в т. ч. через сеть Интернет [2, 9, 10]. К основным компонентам РАИС относятся:

- узлы: системы хранения данных, серверы, рабочие станции, управляемые устройства (в т. ч. относящиеся к Internet of Things (IoT));

- компьютерные сети: локальные и глобальные сети, обеспечивающие связь между узлами и потребителями (в т. ч. принадлежащие различным провайдерам (операторам) связи);

- программное обеспечение: общесистемное и прикладное программное обеспечение (в т. ч. проприетарное и используемое различными поставщиками услуг для сопровождения РАИС).

Особенности построения РАИС и связанные с ними проблемы обеспечения ИБ:

- большие масштабы, в т. ч. охват разных часовых поясов; проблемы – укомплектования и координации между ИБ-командами (группами), в т. ч. проблемы оперативной переброски группы реагирования на инциденты ИБ на конкретную (удаленную) площадку;

- неоднородность ИТ-инфраструктуры (зачастую используются гетерогенные и legacy ИТ-решения, полученные в рамках приобретения различных активов); проблемы – актуальность supply chain кибератак;

- зависимость от поставщиков услуг; проблемы – vendor lock-in.

Дополнительно стоит отметить сложность управления, мониторинга и диагностики РАИС, в т. ч. обнаружения и подтверждения инцидентов ИБ. Для ряда РАИС, существующих больше 10-15 лет, характерны проблемы синхронизации и консистентности накопленных данных, т. к. только с 2009 года начинает набирать популярность специализация по анализу данных [11], и в организациях начинается системная работа с данными.

В части сопровождения РАИС может использоваться одна из следующих моделей организации работ команд, в т. ч. групп реагирования:

- централизованная модель: размещение команды на одной площадке (зачастую круглосуточная посменная восьми – двенадцатичасовая работа персонала, чтобы обеспечить режим сопровождения 24x7x365);

- «следующий за солнцем» (Follow-the-sun (FTS)): размещение команд на нескольких площадках, находящихся в разных часовых поясах (целевая схема – это обеспечить разницу между площадками в восемь – двенадцать часовых поясов, чтобы на каждой площадке была одна рабочая смена);

- гибридная (децентрализованная) модель: размещение команд на нескольких площадках (например: в крупных городах или в городах с наиболее крупными площадками присутствия организации, со своими режимами работы персонала на каждой площадке).

При выборе наиболее подходящей модели оператором РАИС фактически учитываются особенности геоинформационного управления [12].

Факторы, влияющие на реагирование на инциденты ИБ

Основываясь на особенностях построения РАИС предлагаются следующие факторы, которые должны быть учтены при планировании и реализации мер реагирования на инциденты ИБ:

1) Используемая модель организации работы группы реагирования, включая ИТ-персонал, в т. ч. равномерность покрытия ею всех часовых поясов, в которых применяется РАИС (если режим применения не 24x7x365). Принимая во внимание, что для выполнения технических действий по локализации и восстановлению после инцидента ИБ требуется непосредственное участие ИТ-персонала (переконфигурирование РАИС).

2) Используемое количество независимых каналов связи, в т. ч. возможность выделения отдельного канала связи с заданной пропускной способностью для подключения и работы группы реагирования. Принимая во внимание, что именно компьютерные сети выступают одним из основных стоп-факторов в обеспечении работоспособности и обслуживании РАИС (по аналогии с системами хранения данных [13], выступающими неотъемлемой частью РАИС).

3) Целевое временя восстановления (Recovery time objective (RTO)) РАИС, разрешенный (принятый владельцем РАИС) период времени с начала недоступности РАИС до момента восстановления работоспособности. Принимая во внимание, что время простоя является основным параметром для расчета убытков, понесенных организацией из-за кибератаки.

4) Целевая точка восстановления (Recovery point objective (RPO)) РАИС, разрешенный (принятый владельцем РАИС) период времени, за который данные могут быть потеряна (данные с момента последнего резервного копирования до момента восстановления работоспособности). Принимая во внимание, что базы данных и программное обеспечение являются одним из ключевых нематериальных активов организаций [14].

5) Ограничения области реагирования в автоматическом режиме (например: только площадками в удаленных и труднодоступных регионах России или все площадки с РАИС) [15]. Принимая во внимание, что автоматическая локализация инцидента ИБ позволяет сократить степень вовлечения сил групп реагирования, в т. ч. ИТ-персонала.

Заключение

По результатам исследования:

1) Проведен обзор и анализ особенностей построения и сопровождения РАИС, в т. ч. моделей организации работ команд сопровождения (групп реагирования);

2) Предложены факторы, связанные с особенностями построения и сопровождения РАИС, которые должны быть учтены группой реагирования, что позволяет повысить эффективность мероприятий по планированию и реализации мер реагирования на инциденты ИБ, возникающие в РАИС.

Применение результатов настоящего исследования дает положительный эффект в области технических наук (методы и системы защиты информации, ИБ) и представляет наибольший интерес для операторов РАИС, а также для центров ГосСОПКА и координационных центров групп реагирования на компьютерные инциденты (Computer Emergency Response Team Coordination Center (CERT CC)), которые обслуживают такие РАИС.

Направлением развития данного исследования является расширение рассматриваемых мер обеспечения ИБ РАИС.

Литература

1. Кореньков В.В. Карточка проекта фундаментальных и поисковых научных исследований, поддержанного российским научным фондом. Грант РНФ № 19-71-30008. 2019-2022. URL: rscf.ru/project/19-71-30008/ (дата обращения: 26/03/25).

2. Хорошевский В.Г., Курносов М.Г., Мамойленко С.Н. Пространственно-распределенная мультикластерная вычислительная система: архитектура и программное обеспечение // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2011. №1(14). С. 79-84.

3. Ермаков А.С. Цифровая война: понятие, генезис, проблемы защиты национальных интересов государств // Вестник НГУЭУ. 2023. №1. С. 206-221. DOI: 10.34020/2073-6495-2023-1-206-221.

4. Казаков И.Ф., Гулиев Я.И., Бельченков А.А., Рудецкий С.В. Развитие пациент-ориентированных ИТ-сервисов в медицинских организациях // Менеджер здравоохранения. 2022. №S1. С. 63-68. DOI: 10.21045/1811-0185-2022-S-63-68.

5. Соснина Е.Н., Липужин И.А., Крюков Е.В. Перспективы внедрения гексагональных распределительных электрических сетей // Инженерный вестник Дона. 2013. №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/2033.

6. Алексеенко А.А., Подгурская И.Г. Преимущества использования сетей Smart grid и способы реализации в электроэнергетике // Вестник Амурского государственного университета. Серия: Естественные и экономические науки. 2023. №103. С. 55-59. DOI: 10.22250/20730268_2023_103_55.

7. Зарубин М.Ю. Биометрические технологии в ФИНТЕХ: практика и перспективы // Образование и право. 2022. №12. С. 237-239. DOI: 10.24412/2076-1503-2022-12237-239.

8. Калинин В.Н. Заграничный биометрический паспорт: особенности, преимущества и недостатки // Образование. Наука. Научные кадры. 2021. №3. С. 83-93. DOI: 10.24411/2073-3305-2021-3-83-93.

9. George Coulouris, Jean Dollimore, Tim Kindberg. Distributed Systems: Concepts and Design 5th Edition. Pearson, 2011. 1080 p.

10. Abdulaziz A. Al-Zubaidi, Khalid K.A. Abdullah, Muhammed K. Dauda, Mohammed S. Al-Yahya, Mohammed J. Al-Haddad. Distributed Systems: Concepts, Principles, Models and Algorithms // Journal of Early Modern Studies 6(2). 2022. pp. 256-269.

11. Nathan Yau. Rise of the Data Scientist // FlowingData. 2009. URL: flowingdata.com/2009/06/04/rise-of-the-data-scientist/ (дата обращения: 26/03/25).

12. Каганович А.А. Геоинформационное управление пространственно-распределёнными территориальными системами // Информация и космос. 2017. №3. С. 126-134

13. Кузнецов А.В. Организация раздельного хранения данных о событиях безопасности // Вопросы кибербезопасности. 2024. №2(60). С. 22-28. DOI: 10.21681/2311-3456-2024-2-22-28.

14. Куракова Н.Г. Базы данных и информационные системы как часть нематериальных активов ЛПУ // Врач и информационные технологии. 2005. № 5. С. 65-69.

15. Кузнецов А.В. Анализ критериев предоставления мандата на локализацию инцидента информационной безопасности // Инженерный вестник Дона. 2025. №3. URL: ivdon.ru/ru/magazine/archive/n3y2025/9919.

References

1. Koren'kov V.V. Grant RNF № 19-71-30008. 2019-2022. URL: rscf.ru/project/19-71-30008/ (accessed 26/03/25).

2. Horoshevskij V.G., Kurnosov M.G., Mamojlenko S.N. Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika i informatika. 2011. №1(14). pp. 79-84.

3. Ermakov A.S. Vestnik NGUEU. 2023. №1. pp. 206-221. DOI: 10.34020/2073-6495-2023-1-206-221.

4. Kazakov I.F., Guliev Ya.I., Bel'chenkov A.A., Rudeckij S.V. Menedzher zdravoohraneniya. 2022. №S1. pp. 63-68. DOI: 10.21045/1811-0185-2022-S-63-68.

5. Sosnina E.N., Lipuzhin I.A., Kryukov E.V. Inzhenernyj vestnik Dona. 2013. №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/2033.

6. Alekseenko A.A., Podgurskaya I.G. Vestnik Amurskogo gosudarstvennogo universiteta. Seriya: Estestvennye i ekonomicheskie nauki. 2023. №103. pp. 55-59. DOI: 10.22250/20730268_2023_103_55.

7. Zarubin M.Yu. Obrazovanie i pravo. 2022. №12. pp. 237-239. DOI: 10.24412/2076-1503-2022-12237-239.

8. Kalinin V.N. Obrazovanie. Nauka. Nauchnye kadry. 2021. №3. pp. 83-93. DOI: 10.24411/2073-3305-2021-3-83-93.

9. George Coulouris, Jean Dollimore, Tim Kindberg. Distributed Systems: Concepts and Design 5th Edition. Pearson, 2011. 1080 p.

10. Abdulaziz A. Al-Zubaidi, Khalid K.A. Abdullah, Muhammed K. Dauda, Mohammed S. Al-Yahya, Mohammed J. Al-Haddad. Journal of Early Modern Studies 6(2). 2022. pp. 256-269.

11. Nathan Yau. FlowingData. 2009. URL: flowingdata.com/2009/06/04/rise-of-the-data-scientist/ (accessed 26/03/25).

12. Kaganovich A.A. Informaciya i kosmos. 2017. №3. pp. 126-134

13. Kuznetsov A.V. Voprosy kiberbezopasnosti. 2024. №2 (60). pp. 22-28. DOI: 10.21681/2311-3456-2024-2-22-28.

14. Kurakova N.G. Vrach i informacionnye tekhnologii. 2005. № 5. pp. 65-69.

15. Kuznetsov A.V. Inzhenernyj vestnik Dona. 2025. №3. URL: ivdon.ru/ru/magazine/archive/n3y2025/9919.

Дата поступления: 4.03.2025

Дата публикации: 25.04.2025