Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия

С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова

ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа

Аннотация: Рассматривается задача разработки архитектуры динамической системы управления информационной безопасностью информационной системы предприятия, основанной на иерархической организации системы управления, анализе состояния вычислительной системы в информационном пространстве, анализе распространения потока рисков, а также многоагентной организации процессов сбора, анализа данных и принятия решений.

Ключевые слова: защита информации, информационная система предприятия, политика безопасности, управление информационной безопасностью, анализ рисков, архитектура нулевого доверия, многоагентные технологии, нейросетевое прогнозирование.

Введение

Политика безопасности предприятий регламентирует процессы адаптации правил и методов обеспечения информационной безопасности (ИБ) в условиях изменения моделей бизнес-процессов предприятия [1, 2]. Например, сотрудникам предприятия назначаются различные уровни доступа к активам в зависимости от используемых ими устройств связи, их местоположения [3, 4]. Для реализации этого подхода система управления ИБ должна динамически корректировать класс защищенности актива, и, тем самым, изменять права доступа пользователя по мере фиксации изменения уровня риска [5, 6].

Как известно, существует три основных типа мер обеспечения требуемого уровня ИБ: предотвращение, обнаружение и реагирование. Предотвращение означает, что действие или элемент управления предотвращают до того, как потенциальный риск повлияет на достижение цели предприятия [7, 8]. Обнаружение опасного события – это выявление влияния внешней или внутренней среды, которое привело к возникновению опасного события, например, проникновение злоумышленника в сеть

предприятия. Реагирование представляет собой процедуру управления ИБ для минимизации риска.

В настоящее время существуют три основных способа автоматизации управления ИБ вычислительной системы предприятия: автоматический, полуавтоматический и ручной. Автоматизированное управление реализуется на основе заданных политикой безопасности мер и правил управления ИБ. Полуавтоматический процесс предполагает определенный уровень вмешательства администратора сети в процесс управления ИБ. Ручное управление осуществляется полностью администратором сети предприятия. Уровень риска возрастает по мере того, как осуществляется переход от предотвращения к обнаружению и реагированию. Затраты на применяемые меры обеспечения ИБ растут при переходе от автоматизированного к полуавтоматическому и ручному управлению. Несмотря на это, в условиях влияния различных факторов неопределенности на достижение цели предприятия, использование системы автоматического управления ИБ является оправданным [9]. Рассмотрим далее особенности разработки систем управления ИБ в рамках модели нулевого доверия.

Требования к архитектуре системы управления информационной безопасностью в рамках архитектуры нулевого доверия

Чтобы удовлетворить быстро меняющиеся требования к ИБ, необходимо, чтобы система управления ИБ имела гибкую и динамическую архитектуру. Эта архитектура должна позволить нам быстрее внедрять новые методы противодействия угрозам, использовать модели, построенные на методах машинного обучения и адаптироваться к меняющемуся арсеналу угроз [10]. Данная архитектура отличается от традиционной модели обеспечения ИБ на предприятии, которая является бинарной и статической.

В традиционной модели ИБ пользователю обычно либо предоставляется, либо запрещается доступ к активам предприятия (бинарный метод) и после предоставления доступа этот уровень доступа остается постоянным. В рамках модели нулевого доверия динамическая архитектура системы управления заменяет бинарную модель на динамическую многоуровневую модель доверия, которая обеспечивает более детальный контроль над идентификацией и контролем доступа, включая доступ к определенным активам. Это означает, что для отдельного пользователя уровень предоставляемого доступа может динамически меняться с течением времени в зависимости от множества факторов, например, от того, обращается ли пользователь к сети с высокозащищенного управляемого устройства с расширенными возможностями защиты от вредоносного программного обеспечения (ПО) или же с ненадежного устройства.

Гибкость данной архитектуры позволяет воспользоваться доверием, основанным на реальном доказательстве того, что риск угрозы минимизируется. Все устройства связи могут включать некоторый уровень программно-аппаратной безопасности, предназначенный для обеспечения целостности приложений и данных на устройстве, например, двойную аутентификацию.

Данная архитектура базируется на следующих основных методах и принципах:

- Расчет доверия: этот элемент архитектуры управляет идентификацией пользователей и управлением доступом, динамически определяя, следует ли предоставить пользователю доступ к определенным ресурсам и, если да, то какой тип доступа следует предоставить. Расчет основан на таких факторах, как тип клиентского устройства и местоположение пользователя, тип запрашиваемых ресурсов и доступные меры безопасности.

– Зоны безопасности: сетевая инфраструктура разделена на несколько зон безопасности, которые обеспечивают разные уровни защиты. Они варьируются от надежных сетевых зон, содержащих критически важные данные, со строго контролируемым доступом, до ненадежных зон, содержащих менее ценные данные и обеспечивающих более широкий доступ. Связь между зонами может контролироваться, что позволяет гарантировать то, что пользователи могут получить доступ только к тем ресурсам, для которых они авторизованы, и предотвращает компрометацию, а также распространение угрозы по нескольким зонам.

– Сбалансированный контроль: для повышения гибкости и способности восстанавливаться после успешной атаки используемая архитектура управления должна обеспечивать средства превентивного контроля, а также балансировать его с обнаружением и реагированием.

– Периметры пользователей и данных. Признавая, что защита границ корпоративной сети больше не является адекватной, необходимо рассматривать пользователей и данные как дополнительные периметры безопасности и защищать их соответствующим образом. Это означает повышенное внимание к оконечным устройствам и предотвращению использования вредоносного кода, а также повышение осведомленности пользователей и встраивание методов защиты данных в информационные активы предприятия (фрагментация, шифрования и т.п.).

Архитектура иерархической динамической системы управления информационной безопасностью

Рассмотрим далее архитектуру системы управления ИБ, учитывающую ранее рассмотренные особенности построения систем нулевого доверия. В качестве базовой архитектуры выберем иерархическую организацию системы управления с применением многоагентных технологий.

На рис. 1(а) представлена топология вычислительной сети и многоагентной системы сбора и обработки информации, где У1…У3 – узлы обработки информации, КС1…КС3 – каналы обмена данными, А1…А3 – агенты сбора данных о состоянии узлов и каналов обмена данными, БД1…БД3 – базы данных, хранящие журналы состояния узлов обработки информации, АС – агент синхронизации, АА – агент анализа состояния системы обработки информации и управления уровнем защищенности узлов обработки информации.

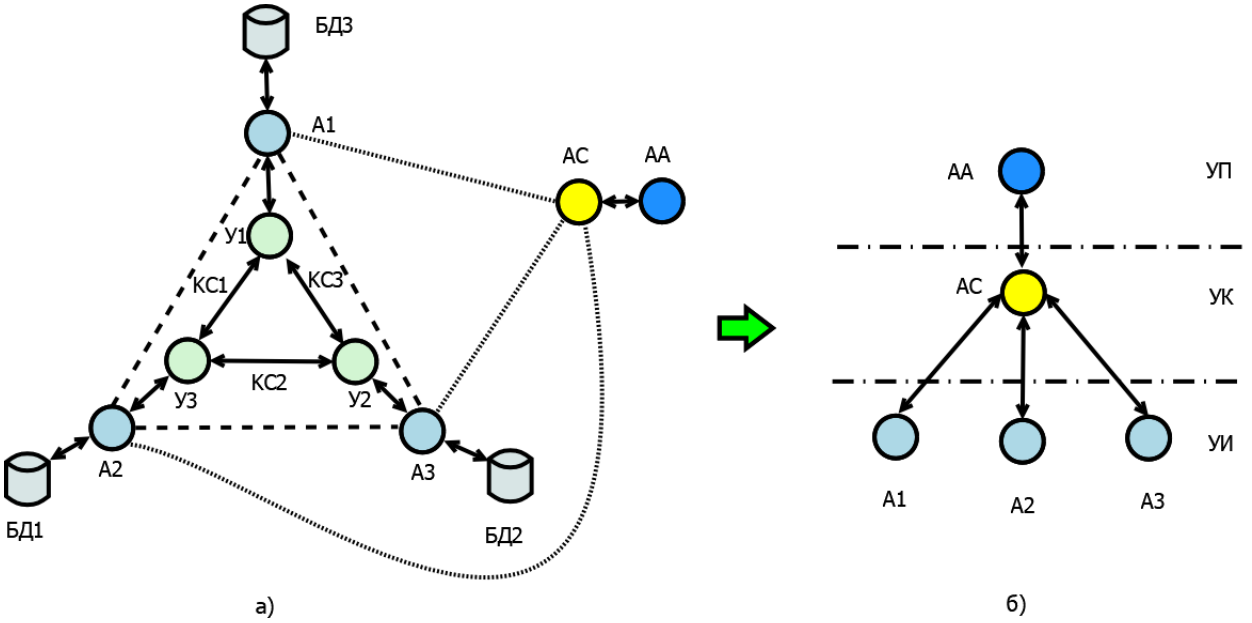

Рис. 1 – Иерархическая архитектура многоагентной системы управления ИБ

На рис. 1 (б) представлена иерархическая архитектура системы управления защитой информации вычислительной системы, где УИ – уровень исполнения, УК – уровень координации, УП – уровень планирования.

Далее рассмотрим особенности реализации элементов системы управления уровнем ИБ на примере вычислительной системы, обеспечивающей доступ к активам предприятия.

На рис. 2 показана вычислительная система в виде графа, включающего узлы доступа (Source), обработки и хранения активов предприятия (Sink). Учитывая, что риски меняются в зависимости от режима работы вычислительной системы, для различных режимов уровень рисков при доступе к активам предприятия также меняется.

На рис. 2 представлена модель максимального потока рисков в вычислительной сети представленной 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 ребер $p_{i,j}$ определяются группой экспертов и являются оценками эффективности средств обеспечения информационной безопасности для данных сегментов сети.

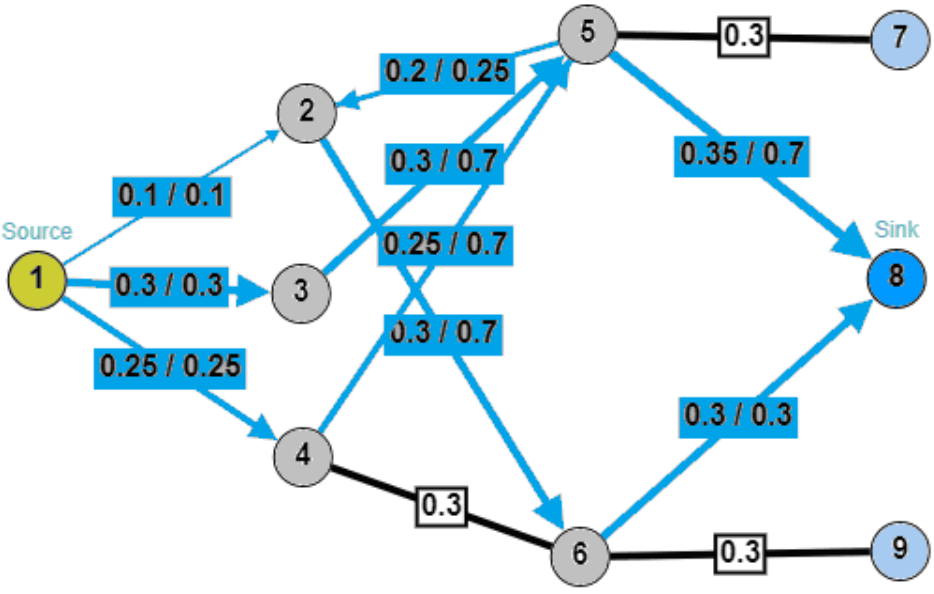

Рис. 2. – Модель вычислительной сети и максимального потока рисков

Как следует из анализа графа G (рис. 2) пути от вершины $v1$ (субъект) через вершины $v3$,$v5$ к вершине $v8$ (актив) и через вершины $v2$, $v6$ имеют высокую пропускную способность для распространения рисков. Тем самым,

при проектировании элементов архитектуры следует в этих вершинах разместить точки применения политики безопасности, например, используя обобщенный шаблон [4].

Нейросетевой модуль назначения рисков активам предприятия

Ценность активов предприятия изменяется со временем, что влияет на изменение оценки рисков для каждого из активов. Это, в свою очередь, требует изменение политик безопасности в точках их применения.

С целью прогнозирования изменения значений уровней рисков для активов предприятия с учетом изменения маршрутов максимальных потоков распространения рисков в информационной сети разработан нейросетевой модуль на базе многослойного персептрона. На основе расчетов потоков рисков выполняется поиск критических участков сети и осуществляется выбор адаптации политик безопасности с применением этого модуля.

Рассмотрим далее пример архитектуры рассматриваемого модуля для графа, представленного на рис. 2. Архитектура нейросетевого модуля (1-3-2-3) представлена на рис. 3, где на вход модуля подаются значения режимов работы информационной сети в виде последовательности скалярных величин $x(t)$, а на выходе модуля определяются значения рисков для заданных активов предприятия

$$R = (r_1(t), r_2(t), r_3(t)).$$

Весовые коэффициенты сети получены в процессе обучения, в качестве алгоритма обучения использовался алгоритм обратного распространения ошибки, ошибка обучения для тестовой выборки равна e = 0,005, а количество шагов обучения равна 26.

В качестве режима работы выбраны часы обслуживания информационной системы предприятия, а риски рассчитываются с учетом экспертных оценок значений рисков для сегментов информационной сети. Далее определяется маршрут максимального потока рисков и определяется

значение риска r_j для заданного i-го актива с учетом изменения его ценности от времени. Эта информация является основой для формирования учебника при обучении нейросетевого модуля.

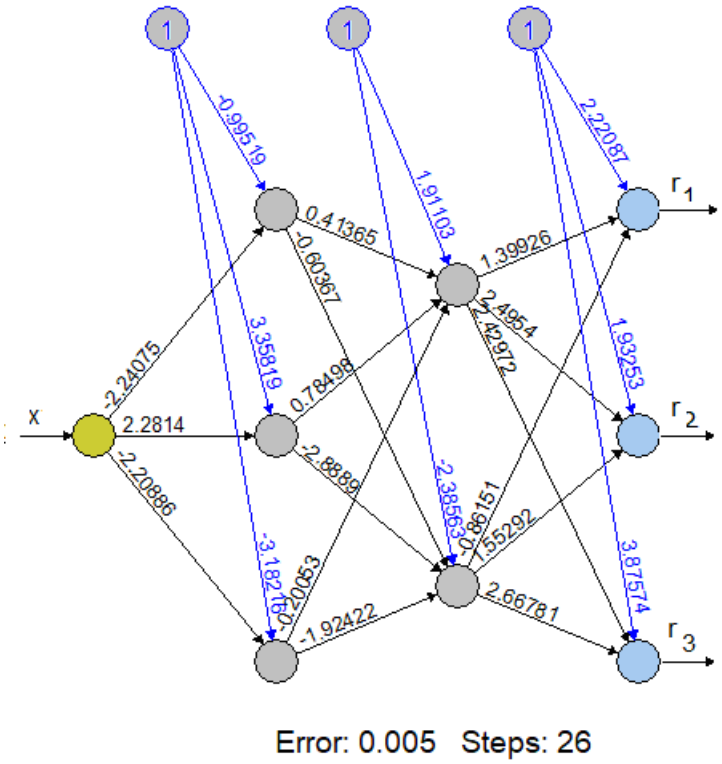

Рис. 3 – Нейросетевой модуль анализа рисков в зависимости от режима работы вычислительной сети

Данный НС-модуль может быть использован в системе управления (см. рис. 1) при проектировании агента анализа состояния системы АА.

В качестве нейронной сети можно использовать, например, рекуррентные нейронные сети, которые позволяют получать прогнозы во времени, однако, при этом необходимо обеспечить заданную устойчивость замкнутой системы управления, что с учетом большой размерности системы и сложностью реализации полной автоматизации процессов управления не является тривиальной задачей. Предполагается, что в рамках дальнейших исследований будут изучены особенности использования в замкнутой системе управления динамических нейронных сетей.

Заключение

Рассмотрены основные требования к архитектурным особенностям современной системы управления информационной безопасностью информационной системой предприятия в рамках модели нулевого доверия. Предложена иерархическая организация системы управления информационной безопасностью вычислительной системы с использование многоагентного подхода. В качестве модуля управления уровнем защищенностью предлагается использовать нейросетевой модуль, на вход которого подается информация о режиме работы информационной системы предприятия, а на выходе формируется прогноз уровня риска для запрашиваемых активов.

Рекомендуемый подход, в отличие от традиционных методов, позволит повысить информационную безопасность предприятия в условиях динамически меняющихся рисков и воздействия различных факторов неопределенности, характерных для внешней среды и влияние различных внутренних угроз на изменение рисков при нарушении целостности активов предприятия.

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

4. Валеев С.С., Кондратьева Н.В. Паттерны проектирования архитектуры нулевого доверия // Инженерный вестник Дона. 2023, №9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8674.

5. 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.

6. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия, Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление», №3 (2023), с. 136-143, doi: 10.18137/Rnu.v9187.23.03.p.136.

7. 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.

8. 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.

9. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization’s information security // Business Informatics. 2017, № 1(39). pp. 68–77.

10. Chollet F., Kalinowski T., Allaire J. J. Deep Learning with R. New York, Manning, 2022. 568 p.

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

4. Valeev S.S., Kondratyeva N.V. Inzhenernyj vestnik Dona, 2023, №9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8674.

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

6. Valeev S.S., Kondratyeva N.V., Guzairov M.B., Melnikov A.V. Vestnik Rossijskogo novogo universiteta. Seriya “Slozhny`e sistemy`: modeli, analiz i upravlenie”, 2023, №3, pp. 136-143.

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

8. 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.

9. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization’s information security. Business Informatics. 2017. № 1 (39). pp. 68–77. DOI: 10.17323/1998-0663.2017.1.68.77

10. Chollet F., Kalinowski T., Allaire J. J. Deep Learning with R. New York, Manning, 2022. 568 p.