Инженерный вестник Дона, №12 (2025)
ivdon.ru/ru/magazine/archive/n12y2025/10592

Защита объектов от угроз информационной безопасности на основе использования их интеллектуальных цифровых двойников

Д.С. Горин, Р.Р. Шатовкин

МИРЭА – Российский технологический университет, Москва

Аннотация: В статье сформулировано обоснованное определение интеллектуального цифрового двойника объекта защиты от угроз информационной безопасности и определены основные этапы его разработки. Разработаны теоретико-множественные модели объекта защиты и интеллектуального цифрового двойника, позволяющие выявить их идентичные составляющие и отличительные компоненты, определяющие механизм противодействия угрозе. На основе положений теории конфликта выявлены отношения между объектом защиты и угрозой в случае отсутствия интеллектуального цифрового двойника, а также при наличии интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности. Полученные макродинамические модели рассмотренных ситуаций позволяют обосновать целесообразность реализации механизма защиты объекта от угроз информационной безопасности на основе использования его интеллектуального цифрового двойника и позволяют оценить общий эффект от его применения.

Ключевые слова: информационная безопасность, объект защиты, интеллектуальный цифровой двойник, угроза, теоретико-множественная модель, теория конфликта, макродинамическая модель.

Введение

Результаты анализ рынка информационной безопасности показали, что в настоящее время идет активное замещение традиционного комплексного применения программных средств обеспечения информационной безопасности от разных производителей соответствующими экосистемами одного поставщика.

В работах [1, 2] достаточно подробно рассмотрены достоинства такого подхода, как нового эволюционного витка развития средств обеспечения информационной безопасности.

Типовой состав представленных на рынке экосистем (например, от компаний Fortinet, Palo Alto Networks, «Лаборатория Касперского», Positive Technologies, BI.ZONE и т.д.) включает в себя как классические решения для обеспечения сетевой и хостовой безопасности, песочницы, анализаторы трафика, системы управления уязвимостями, так и решения для обеспечения

безопасности облачных инфраструктур, удаленной работы, технологий контейнеризации, IoT-устройств и OT-инфраструктур, а также платформы управления и реагирования на киберинциденты, выявления аномалий, управления аналитикой киберугроз и решения, дополненные технологиями машинного обучения и искусственного интеллекта [3–5].

Однако, не смотря на значительное расширение возможностей в обеспечении информационной безопасности и определенное повышение качества защиты объектов, существенного прорыва с применением экосистем в этом направлении не произошло.

Одной из основных причин этого может быть сам подход к организации защиты объектов от угроз информационной безопасности: применяемые средства вне зависимости от формы организации их взаимодействия (в рамках единой платформы как в экосистемах или в виде комплексного использования разрозненных средств) ориентированы на определенный вид угрозы. Как следствие, сначала возникает угроза нового типа, и только потом появляется средство, способное противостоять ей. То есть, средства обеспечения информационной безопасности вне зависимости от формы организации их взаимодействия всегда выступают в роли «догоняющего». При этом превентивность мер возможна лишь в рамках предполагаемого направления развития конкретной угрозы, что на практике зачастую оказывается неэффективным. Это подтверждается наблюдающимся ростом количества преступлений в IT-сфере [6–8].

Альтернативным вариантом организации защиты объектов от угроз информационной безопасности и, как следствие, построения экосистемы информационной безопасности является определение ее состава и функционального назначения элементов с учетом назначения, особенностей функционирования и характерных уязвимостей самих защищаемых объектов. Тогда роль «догоняющего» в развитии средств обеспечения информационной

безопасности меняется на роль «обороняющего» защищаемый объект вне зависимости от вида угрозы.

Цель статьи – определение сущности и этапов разработки интеллектуального цифрового двойника объекта, защищаемого от угроз информационной безопасности, обоснование целесообразности реализации механизма защиты на его основе.

Определение сущности и этапов разработки интеллектуального цифрового двойника объекта защиты от угроз информационной безопасности

В соответствии с ГОСТ Р 57700.37–2021 «Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения», принятым в России в 2021 году, под цифровым двойником изделия понимается система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями.

В свою очередь, цифровая модель изделия – это система математических и компьютерных моделей, а также электронных документов изделия, описывающая структуру, функциональность и поведение разрабатываемого или эксплуатируемого изделия на различных стадиях жизненного цикла, для которой на основании результатов цифровых и (или) иных испытаний по ГОСТ 16504–81 «Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения» выполняется оценка соответствия предъявляемым к изделию требованиям.

Под интеллектуальным цифровым двойником, в широком смысле, понимается двойник, использующий различные методы (машинного обучения, искусственного интеллекта, мягких вычислений и т.д.) для анализа и прогноза поведения объекта в разнообразных условиях в реальном масштабе времени [9]. В контексте такого понимания роли двойника, он находит широкое применение в строительстве, промышленности, энергетике и т.д. [10, 11].

Однако, в области информационной безопасности традиционная роль интеллектуального цифрового двойника защищаемого объекта не получила широкого практического применения.

В то же время, вполне правомерно предположить, что если существует возможность с использованием интеллектуального цифрового двойника проводить исследования поведения реального объекта-прототипа в изменяющихся условиях, то с помощью этого же инструмента возможен анализ самих условий при заданных фиксированных характеристиках и функционале объекта.

На этом предположении и основан предлагаемый подход к защите объектов от угроз информационной безопасности: цифровой двойник защищаемого объекта воспроизводит его функционал с присущими потенциальными уязвимостями, имитируя процессы внутренней обработки информации и взаимодействие с внешней средой, и анализирует все внешние воздействия на предмет нестандартного поведения или негативного влияния на внутренние процессы. В случае, если нестандартных отклонений и негативного влияния не зафиксировано, к взаимодействию с внешней средой подключается сам защищаемый объект. Однако, если выявлено отклонение или негативное влияние, то оно анализируется, и определяется вид угрозы. Сам объект защиты в этом случае до взаимодействия с внешней средой не допускается.

Таким образом, под *интеллектуальным цифровым двойником объекта защиты от угроз информационной безопасности* будем понимать двойник, воспроизводящий функционал защищаемого объекта с присущими ему потенциальными уязвимостями, имитирующий процессы внутренней обработки информации и взаимодействия с внешней средой, и способный с использованием различных методов (машинного обучения, искусственного интеллекта, мягких вычислений и т.д.) осуществлять анализ внешних воздействий на предмет содержания в них угроз объекту защиты.

Создание такого двойника требует комплексного подхода и сочетания нескольких технологических компонентов, включающих имитационные модели защищаемых объектов (программные средства, позволяющие создавать полнофункциональную симуляцию объектов и их взаимодействие с внешним миром), аналитические инструменты (программные средства для обработки и анализа входных воздействий, в том числе с применением методов искусственного интеллекта и машинного обучения), общее хранилище данных о потенциально возможных угрозах, а также интерфейсы взаимодействия (программные средства для представления данных в удобном для пользователя и защищаемого объекта виде), объединенные в рамках одной цифровой платформы – экосистемы информационной безопасности.

В основе создания интеллектуального цифрового двойника объекта защиты от угроз информационной безопасности следует использовать метод «белого ящика», который обеспечивает максимально полное и точное моделирование реального объекта. Конечно, такой подход требует высокой квалификации специалистов, значительных временных и вычислительных ресурсов. Однако, он позволяет создать цифровую копию, идентичную реальному объекту, с требуемым уровнем детализации его состава, протекающих в нем процессов и выполняемого им функционала, а также с заданной точностью воспроизведения его параметров и характеристик.

Интеллектуальный цифровой двойник объекта защиты от угроз информационной безопасности, исходя из его назначения, следует разрабатывать в соответствии со следующими этапами:

1. Исследование объекта защиты. На этом этапе производится детальное описание объекта: определяется его назначение, состав и функции; режимы работы; потенциальные уязвимости и характерные угрозы; внутренние процессы, протекающие в объекте, и типовые стандартные внешние воздействия на него; параметры и характеристики объекта.

2. Создание имитационной модели объекта защиты. На этом этапе непосредственно производится создание цифровой копии объекта защиты.

3. Определение перечня аналитических инструментов и их реализация. На этом этапе в зависимости от назначения и функций объекта защиты, а также его потенциальных уязвимостей и характерных угроз разрабатываются алгоритмы обработки и анализа входных воздействий, делающие цифровой двойник объекта интеллектуальным. Производится программная реализация полученных алгоритмов.

4. Определение интерфейсов взаимодействия и их реализация. На этом этапе разрабатываются алгоритмы взаимодействия интеллектуального цифрового двойника с пользователем и объектом защиты, а также реализующие их программы.

Таким образом, с учетом специфики области информационной безопасности и роли цифрового двойника в обеспечении защиты объекта-прототипа дано обоснованное определение интеллектуального цифрового двойника объекта защиты от угроз информационной безопасности и определены основные этапы его разработки.

Обоснование целесообразности реализации механизма защиты объекта от угроз информационной безопасности на основе использования его интеллектуального цифрового двойника

Представим объект защиты от угроз информационной безопасности O в виде теоретико-множественной модели:

$$O = \{F_O, P_O, V_O, g_O\}, \quad (1)$$

где F_O – множество функций объекта; P_O – множество внутренних процессов обработки информации; V_O – множество потенциальных уязвимостей объекта; g_O – интерфейс взаимодействия с пользователем.

Множество функций объекта F_O:

$$F_O = \{f_{O1},...,f_{On}\}, \quad (2)$$

где количество функций n определяется назначением конкретного объекта защиты.

Множество внутренних процессов обработки информации в объекте P_O:

$$P_O = \{p_{O1},...,p_{Om}\}, \quad (3)$$

где количество процессов m определяется назначением конкретного объекта защиты.

Множество потенциальных уязвимостей объекта V_O:

$$V_O = \{v_{O1},...,v_{Ok}\}, \quad (4)$$

где количество уязвимостей k определяется реализацией конкретного объекта защиты.

В свою очередь, исходя из сформулированного определения понятия интеллектуального цифрового двойника T объекта защиты от угроз информационной безопасности, его можно представить в виде:

$$T = \{M, A_T, G_T\}, \quad (5)$$

где

$$M = \{F_T, P_T, V_T\}; \quad (6)$$

M – имитационная модель объекта; F_T – множество функций двойника; P_T – множество внутренних процессов обработки информации в двойнике; V_T – множество учтенных в двойнике потенциальных уязвимостей объекта-прототипа; A_T – множество аналитических инструментов; G_T – множество интерфейсов взаимодействия с пользователем и объектом защиты.

С учетом применения метода «белого ящика» при создании точной цифровой копии объекта защиты правомерно предположить, что: $F_T \equiv F_O$, $P_T \equiv P_O$, $V_T \equiv V_O$. То есть имитационная модель объекта практически полностью идентична реальному объекту защиты: $M \equiv O$.

Определим множество воздействий внешней среды I как:

$$I = \{I_+, I_-\}, \quad (7)$$

где I_{O+} – множество стандартных ожидаемых воздействий; I_{O-} – множество негативных воздействий (угроз).

Можно ожидать, что если интеллектуальный цифровой двойник T способен с использованием множества аналитических инструментов A_T распознать негативное воздействие I_{O-}, то реальный объект O этого сделать не сможет, и, как следствие, будет подвергнут угрозе.

Используя теорию конфликта, рассмотрим отношения, существующие между сторонами O и I_{O-} для случаев:

– отсутствия интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности;

– наличия интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности.

В случае отсутствия интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности имеет место отношение «взаимное противодействие» между сторонами конфликта O и I_{O-}, которое можно представить в виде частного отношения «одностороннее противодействие» – разновидности противодействия, при котором одна сторона оказывает негативное влияние на другую сторону, а другая сторона не оказывает никакого влияния на первую [12].

Таким образом, объект защиты подвергнут угрозе без возможности противодействия.

Формально отношение «одностороннее противодействие» между сторонами O и I_{O-} можно представить как:

$$S_{-0} : \left(\partial E_O / \partial E_I < 0\right) \wedge \left(\partial E_I / \partial E_O = 0\right), \quad (8)$$

где знак «∧» – логическое «И»; $\partial E_O / \partial E_I$ и $\partial E_I / \partial E_O$ – частные производные, значения которых характеризуют интенсивность влияния сторон друг на друга, а знаки – направления влияния.

В случае наличия интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности, замещающего реальный объект, имеет место отношение «нейтралитет», которое характеризуется тем, что рассматриваемые элементы сторон не оказывают непосредственного влияния на функционирование друг друга [12].

Таким образом, объект защиты не участвует в прямом взаимодействии с угрозой.

Формально отношение «нейтралитет» между сторонами *O* и I_{O-} можно представить, как:

$$S_{00} : \left(\partial E_O / \partial E_I = 0\right) \wedge \left(\partial E_I / \partial E_O = 0\right). \quad (9)$$

Также, используя теорию конфликта, рассмотрим отношения, существующие между сторонами *T* и I_{O-}. Имеет место отношение «взаимное противодействие», которое можно представить в виде частного отношения «антагонизм» – предельной степени противодействия в конфликте, при которой достижение цели одной стороной исключает достижение цели другой стороной (компромисс невозможен) [12].

Формально отношение «антагонизм» между сторонами *T* и I_{O-} можно представить как:

$$S_{--}^{ан} : \left[\left(\partial E_T / \partial E_I < 0\right) \wedge \left(\partial E_I / \partial E_T < 0\right)\right] \wedge \left[max\, E_T \Leftrightarrow (E_I = 0), max\, E_I \Leftrightarrow (ET_T = 0)\right], \quad (10)$$

где символ $\Leftrightarrow$ означает взаимное соответствие (например, выражение «$T \Leftrightarrow I$» означает, что «*T*» влечет за собой «*I*» и «*I*» влечет за собой «*T*»).

В свою очередь, рассмотрим отношения, существующие между сторонами *O* и *T*. Имеет место отношение «взаимное содействие», которое

можно представить в виде частного отношения «единство» – предельной степени содействия, при которой цели сторон сливаются в одну общую цель [12].

Формально отношение «единство» между сторонами O и T можно представить, как:

$$S_{++}^{ед} : \partial E_O / \partial E_T = 1. \quad (11)$$

На рис. 1 и рис. 2 представлены макродинамические модели, иллюстрирующие рассматриваемый конфликт, соответственно, для случая отсутствия интеллектуального цифрового двойника, и для случая наличия интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности.

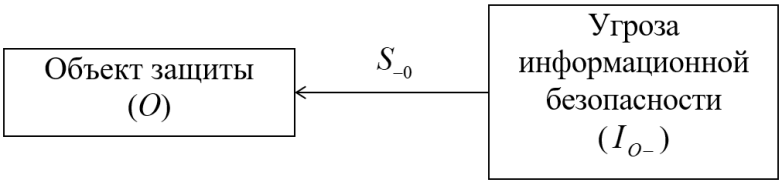

Рис. 1. – Макродинамическая модель конфликта для случая отсутствия интеллектуального цифрового двойника в системе защиты

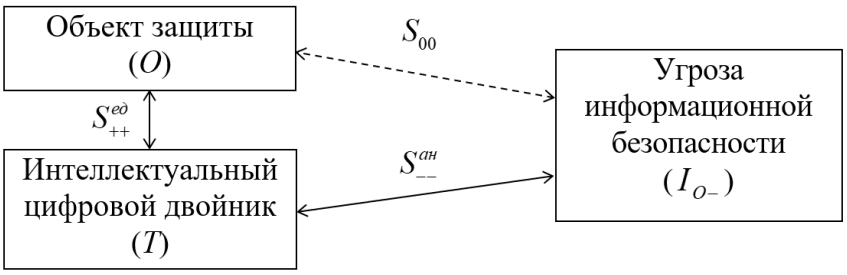

Рис. 2. – Макродинамическая модель конфликта для случая наличия интеллектуального цифрового двойника в системе защиты

Представленные рисунки позволяют наглядно оценить целесообразность реализации механизма защиты объекта от угроз информационной безопасности на основе использования его интеллектуального цифрового двойника, а также общий эффект от его применения.

Заключение

В результате проведенных исследований:

1. Сформулировано обоснованное определение интеллектуального цифрового двойника объекта защиты от угроз информационной безопасности и определены основные этапы его разработки.

2. Разработаны теоретико-множественные модели объекта защиты и интеллектуального цифрового двойника, позволяющие выявить их идентичные составляющие и отличительные компоненты, определяющие механизм противодействия угрозе.

3. На основе положений теории конфликта выявлены отношения между объектом защиты и угрозой в случае отсутствия интеллектуального цифрового двойника, а также при наличии интеллектуального цифрового двойника в системе защиты объекта от угроз информационной безопасности. Полученные макродинамические модели рассмотренных ситуаций позволяют обосновать целесообразность реализации механизма защиты объекта от угроз информационной безопасности на основе использования его интеллектуального цифрового двойника.

Литература

1. Ахрамеева К.А., Вистунов С.С. Сравнительный анализ рынка экосистем информационной безопасности // Экономика и качество систем связи, 2024, № 3. С. 119–126.

2. Ревенко Г. Полезность экосистемного подхода к кибербезопасности // URL: safe-surf.ru/specialists/article/5309/687698/?ysclid=mgqr0srzdf134524088.

3. Зенков А.В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.

4. Курейчик В.М., Сахарова О.Н., Пирожков С.С. Угрозы в области хранения данных // Инженерный вестник Дона, 2021, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111.

5. Чибинев Н.Н., Ляшенко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона, 2024, № 7. URL: ivdon.ru/ru/magazine/ archive/n7y2024/9323.

6. Киберпреступность в России: 765 тысяч случаев за 2024 год // URL: itsec.ru/news/kiberprestupnost-v-rossii-765-tisiach-sluchayev-za-2024-god.

7. Сколько киберпреступлений зафиксировано в России в 2025 году и какой от них ущерб? - 18 июня 2025 | ФОНТАНКА.ру // URL: fontanka.ru/ 2025/06/18/75604451/?ysclid=mgalbc1qnf500542194.

8. Киберпотери российской экономики – Медиаплатформа МирТесен // URL: nayavu.mirtesen.ru/blog/ 43689945896/ Kiberpoteri-rossiyskoy-ekonomiki.

9. Как устроены цифровые двойники: этапы разработки и примеры использования // URL: softline.ru/about/blog/kak-ustroeny-tsifrovye-dvoyniki-etapy-razrabotki-i-primery-ispolzovaniya.

10. Reid J.B., Rhodes D.H. Digital system models: An investigation of the non-technical challenges and research needs. Conference on Systems Engineering Research, Systems Engineering Advancement Research Initiative. Massachusetts Institute of Technology, 2016. 10 p.

11. Grieves M. Digital twin: Manufacturing excellence through virtual factory replication. Digital Twin White Paper, 2014. 7 p.

12. Новосельцев В.И., Тарасов Б.В. Системная теория конфликта: издание второе, исправленное и дополненное / Под ред. В.И. Новосельцева. М: Издательство «Майор», 2012. 528 с.

References

1. Akhrameeva K.A., Vistunov S.S. Ekonomika i kachestvo sistem svyazi, 2024, № 3. pp. 119–126.

2. Revenko G. Poleznost ekosistemnogo podkhoda k kiberbezopasnosti [The usefulness of an ecosystem approach to cybersecurity]. URL: safe-surf.ru/specialists/article/5309/687698/?ysclid=mgqr0srzdf134524088.

3. Zenkov A.V. Informatsionnaya bezopasnost i zashchita informatsii [Information security and information protection]. M.: Yurait. 2023. 108 p.

4. Kureichik V.M., Sakharova O.N., Pirozhkov S.S. Inzhenernyj vestnik Dona, 2021, № 7 URL: ivdon.ru/ru/magazine/archive/n7y2021/7111.

5. Chibinev N.N., Lyashenko N.V. Inzhenernyj vestnik Dona, 2024, № 7 URL: ivdon.ru/ru/magazine/ archive/n7y2024/9323.

6. Kiberprestupnost v Rossii: 765 tisyach sluchaev za 2024 god [Cybercrime in Russia: 765,000 cases in 2024]. URL: itsec.ru/news/kiberprestupnost-v-rossii-765-tisiach-sluchayev-za-2024-god.

7. Skolko kiberprestuplenii zafiksirovano v Rossii v 2025 godu i kakoi ot nikh ushcherb? [How many cybercrimes were recorded in Russia in 2025 and what damage did they cause?]. 18 iyunya 2025. FONTANKA.ru. URL: fontanka.ru/2025/ 06/18/75604451/?ysclid=mgalbc1qnf500542194.

8. Kiberpoteri rossiiskoi ekonomiki. [Cyber losses of the Russian economy] Mediaplatforma MirTesen. URL: nayavu.mirtesen.ru/blog/ 43689945896/ Kiberpoteri-rossiyskoy-ekonomiki.

9. Kak ustroeni tsifrovie dvoiniki: etapi razrabotki i primeri ispolzovaniya [How digital twins work: development stages and usage examples]. URL: softline.ru/about/blog/kak-ustroeny-tsifrovye-dvoyniki-etapy-razrabotki-i-primery-ispolzovaniya.

10. Reid J.B., Rhodes D.H. Conference on Systems Engineering Research, Systems Engineering Advancement Research Initiative. Massachusetts Institute of Technology, 2016. 10 p.

11. Grieves M. Digital twin: Manufacturing excellence through virtual factory replication. Digital Twin White Paper, 2014. 7 p.

12. Novoseltsev V.I., Tarasov B.V. Sistemnaya teoriya konflikta: izdanie vtoroe, ispravlennoe i dopolnennoe [System Theory of Conflict: Second Edition, Revised and Expanded]. Pod red. V.I. Novoseltseva. M: Izdatelstvo «Maior», 2012. 528 p.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 15.10.2025 Дата публикации: 27.11.2025