Инженерный вестник Дона, №10 (2025)
ivdon.ru/ru/magazine/archive/n10y2025/10482

Реализация экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов

Д.С. Горин, Р.Р. Шатовкин

МИРЭА – Российский технологический университет, Москва

Аннотация: В статье проведен краткий анализ мер информационной безопасности, позволивший обосновать ведущую роль в современных условиях технических мер защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем. Анализ роста показателей кибепреступности в России выявил моральную устарелость существующего комплексного подхода к защите элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем, и определил необходимость, своевременность и актуальность создания и применения экосистемы информационной безопасности. Анализ существующих единичных решений по созданию и применению экосистем информационной безопасности выявил необходимость применения интеллектуальных цифровых двойников защищаемых объектов для нейтрализации угроз информационной безопасности. На основе проведенного анализа определены особенности реализации экосистемы информационной безопасности с использованием интеллектуальных цифровых двойников элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем.
Ключевые слова: экосистема информационной безопасности, интеллектуальный цифровой двойник, угроза информационной безопасности, анализ уязвимостей, мониторинг и обнаружение угроз, защита и предотвращение атак.

Введение

Стремительное развитие цифровых технологий обусловливает необходимость постоянного совершенствования методов и средств защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем от угроз информационной безопасности.

Такие методы и средства составляют основу информационной безопасности.

Выделяется три главных компонента информационной безопасности [1]:

1. Технические меры – комплекс мероприятий, подразумевающий использование цифровых технологий, включающих методы, программные и аппаратные средства, для защиты компьютерных систем, цифровых систем, систем сотовой связи и их пользователей от угроз информационной

безопасности (антивирусные программы, системы обнаружения предотвращения вторжений, шифрование данных и т.д.).

2. Организационные меры – правила и процедуры, которые регулируют использование компьютерных систем, цифровых систем и систем сотовой связи пользователями (политики безопасности, стандарты и рекомендации, которые определяют порядок работы пользователей с информацией).

3. Правовые меры – законы, нормативные и правовые акты, которые регламентируют порядок использования компьютерных систем, цифровых систем и систем сотовой связи пользователями:

– Федеральный закон № 126-ФЗ «О связи» от 07.07.2003 г.;

– Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г.;

– Федеральный закон № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» от 01.04.2025 г.;

– Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011 г.;

– Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г.;

– различные отраслевые и ведомственные нормативные документы и т.д.

При этом важнейшим аспектом эффективной реализации рассмотренных компонент информационной безопасности является наличие подготовленного пользователя.

В рамках проводимого исследования основное внимание уделяется техническим мерам информационной безопасности как наиболее динамичным в развитии и совершенствовании по сравнению с другими ее компонентами системы безопасности.

Анализ технических средств и методов информационной безопасности

Программными и аппаратными средствами, обеспечивающими технические меры информационной безопасности, на сегодняшний день являются [2, 3]:

1. Инструменты для анализа уязвимостей:

– сканеры уязвимостей – помогают выявлять слабые места в системе, которые могут быть использованы злоумышленниками; проводят автоматический анализ сетевых устройств, серверов и приложений на предмет известных уязвимостей; играют ключевую роль в процессе управления уязвимостями, позволяя своевременно обнаруживать и устранять потенциальные угрозы (например, Nessus, OpenVAS);

– средства статического и динамического анализа кода – анализируют исходный код приложений на предмет уязвимостей, таких как SQL-инъекции или XSS (межсайтовый скриптинг); статический анализ проводится без выполнения кода, что позволяет выявлять уязвимости на ранних стадиях разработки; динамический анализ проводится во время выполнения приложения, что позволяет обнаруживать уязвимости, которые могут возникнуть только в реальных условиях эксплуатации (например, SonarQube, Burp Suite).

2. Инструменты для мониторинга и обнаружения угроз:

– системы обнаружения и предотвращения вторжений IDS/IPS (Intrusion Detection System / Intrusion Prevention System) – мониторят сетевой трафик и события на предмет подозрительной активности и могут автоматически блокировать потенциальные угрозы; IDS обнаруживает подозрительную активность и уведомляет администратора; IPS может автоматически принимать меры для блокировки угроз (например, Snort, Suricata);

– SIEM-системы (Security Information and Event Management) – собирают и анализируют данные из различных источников для выявления

аномалий и корреляции событий; играют ключевую роль в обеспечении ситуационной осведомленности и позволяют своевременно реагировать на инциденты безопасности (например, Splunk, ELK Stack (Elasticsearch, Logstash, Kibana)).

3. Инструменты для защиты и предотвращения атак:

– антивирусные и антишпионские программы – защищают системы от вредоносного программного обеспечения, включая вирусы, трояны и шпионские программы; антивирусные программы сканируют файлы и процессы на наличие вредоносного кода; антишпионские программы обнаруживают и удаляют шпионское программное обеспечение, которое может собирать конфиденциальную информацию (например, Kaspersky, Malwarebytes);

– брандмауэры (Firewall) – контролируют входящий и исходящий сетевой трафик на основе заданных правил безопасности; играют ключевую роль в защите сетей от несанкционированного доступа и помогают предотвращать распространение вредоносного программного обеспечения (например, pfSense, Cisco ASA).

4. Инструменты для реагирования на инциденты и восстановления:

– платформы для управления инцидентами – помогают организовать и автоматизировать процесс реагирования на инциденты, включая расследование и устранение последствий; играют ключевую роль в обеспечении оперативного реагирования на инциденты и минимизации их последствий (например, TheHive, IBM Resilient);

– инструменты для резервного копирования и восстановления – позволяют создавать резервные копии данных и систем, а также восстанавливать их в случае утраты или повреждения (например, Veeam, Acronis).

Использование этих инструментов в комплексе позволяет защитить компьютерные системы, цифровые системы, системы сотовой связи и их пользователей от различных угроз информационной безопасности.

Функционирование рассмотренных средств основано на применении математических методов из области [4–6]:

1. Методы криптографии:

– использование теории чисел – для разработки криптографических алгоритмов (например, алгоритмы с открытым ключом RSA);

– применение комбинаторных методов – для анализа и проектирования шифров (например, симметричные алгоритмы шифрования AES);

– использование хеш-функций – для создания «отпечатков» данных, обеспечивающих их целостность (например, SHA-256, SHA-3).

2. Методы статистики:

– анализ рисков и оценка вероятности возникновения угроз информационной безопасности – для анализа вероятности возникновения конкретной угрозы и ее потенциальных последствий; помогает классифицировать и приоритезировать риски;

– анализ исторических инцидентов – для исследования данных предыдущих инцидентов безопасности и выявления типичных сценариев атак и их возможных последствий; позволяет прогнозировать будущие угрозы;

– анализ аномалий – для выявления отклонений от нормального поведения, которые могут указывать на вторжение или другие угрозы безопасности.

3. Методы моделирования:

– математическое моделирование – позволяет моделировать сетевые атаки, создавать модели систем и сетей для оценки уязвимостей и оптимизации конфигурации систем защиты;

– систематические методы (например, STRIDE, PASTA, Attack Trees) – используют математические структуры (графы, деревья) для выявления и документирования потенциальных угроз системе на основе ее архитектуры.

4. Методы машинного обучения:

– обучение с учителем – использование размеченных данных для обучения модели в интересах классификации угроз;

– обучение без учителя – алгоритмы ищут скрытые структуры в данных в интересах обнаружения аномалий, таких как необычная активность в сети, которая может указывать на потенциальную угрозу;

– глубокое обучение – использует нейронные сети с множеством слоев для анализа сложных данных; применяется для анализа больших объемов логов и обнаружения сложных атак, которые трудно выявить традиционными методами.

Однако, злоумышленники постоянно совершенствуют методы и средства атак, нейтрализуя существующую защиту. В этом случае применяемые методы и средства выступают в роли «догоняющего», не обеспечивая превентивность технических мер защиты.

Анализ роста показателей кибепреступности в России

Так, за 2024 год в России зарегистрировано 765,4 тысячи преступлений, совершенных с использованием информационных технологий и интернета. Это на 13,1 % больше, чем в 2023 году [7].

С января по май 2025 года зафиксировано более 308 тысяч преступлений в IT-сфере. Общий ущерб за этот период от действий киберпреступников превысил 81 миллиард рублей [8].

При этом, основными видами угроз информационной безопасности по данным исследования киберпреступности в России и ее влияния на экономику страны являются: программы-вымогатели, DDos-атаки, фишинг (рис. 1) [9].

Ущерб организациям от угроз информационной безопасности по секторам экономики проиллюстрирован на рис. 2 [9].

Одной из основных причин такого положения является методологическая, концептуальная и аппаратная разрозненность, а также слабая интеллектуализация средств защиты. Их комплексного использования на сегодняшний день

оказывается недостаточным для гарантированной защиты систем и их пользователей от угроз информационной безопасности.

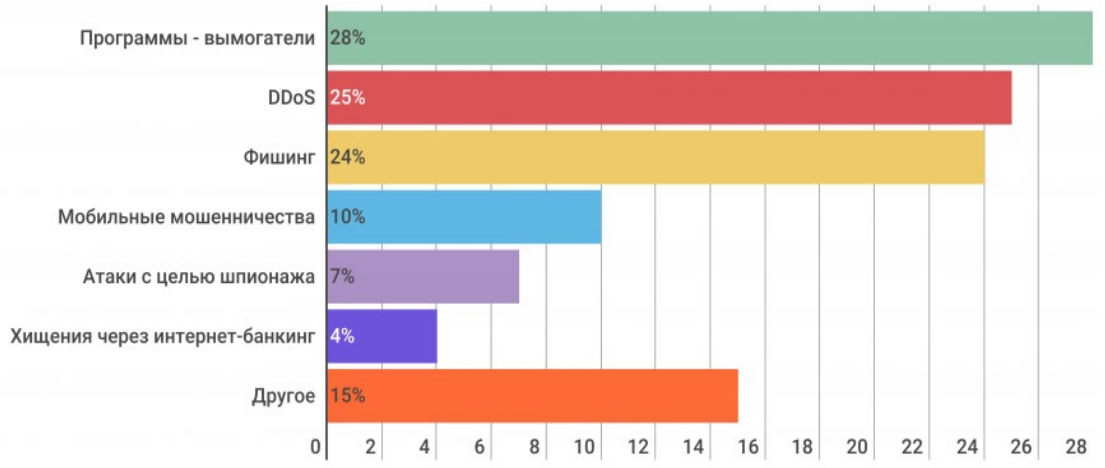

Рис. 1. – Процентное соотношение видов угроз информационной безопасности

Рис. 2. – Ущерб организациям от угроз информационной безопасности по секторам экономики

Логичным и технологически обоснованным решением в данном случае является переход от комплексного использования средств защиты к их применению в рамках единой платформы – экосистемы информационной безопасности с привлечением методов построения интеллектуальных систем для анализа, предотвращения и обезвреживания кибератак.

Анализ существующих решений по созданию экосистем информационной безопасности и обоснование актуальности применения для этого интеллектуальных цифровых двойников защищаемых объектов

На сегодняшний день прослеживается четкая тенденция создания и внедрения экосистем информационной безопасности для защиты организаций, в первую очередь, от кибератак.

Так, созданием и продвижением на рынке экосистем информационной безопасности занимаются компании: «BI.ZONE» [10], R-Vision EVO [11], «Лаборатории Касперского» [12], «Газинформсервис» [13].

Большая часть из этих компаний реализует свои услуги безопасности типа MSSP (Managed Security Service Providers) или же SECaaS (Security-as-a-Service) в виде сервисов с помощью облачной или гибридной модели экосистемы информационной безопасности [14].

Готовые решения уже развернуты на их серверах и остается только подключить к своей сети пользователя.

Кроме того, компании-поставщики могут предоставить пользователю решение, которое ему необходимо, в виде локальной экосистемы. Основная проблема такого подхода заключается в том, что в случае, если пользователь (организация с локальной экосистемой) будет подвержен кибератаке, то ему придется самому решать проблемы и устранять последствия, вызванные этой атакой. А компания-поставщик отвечает только за установку оборудования и предоставление решения по безопасности [14].

Несмотря на новый формат предоставляемых услуг по обеспечению информационной безопасности, методы ее обеспечения во многом остались прежними, а вместо комплексного применения существующих средств наблюдается их интеграция в рамках единой платформы. При этом интеллектуализация методов и средств защиты наблюдается лишь в рамках решения частных задач (например, обнаружение угроз в компьютерных

системах, использование ассистента пользователя в системах сотовой связи), без применения методов построения интеллектуальных систем и методов искусственного интеллекта на глобальном уровне.

Такое положение обусловливает острую необходимость разработки соответствующих концепции и методологии создания и применения экосистемы информационной безопасности, а также математического, алгоритмического и программного обеспечения на их основе с применением методов построения интеллектуальных систем и методов искусственного интеллекта на глобальном уровне.

Поэтому своевременным, актуальным и практически важным является вопрос разработки моделей и методов создания и применения, а также средств реализации экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов, позволяющих нейтрализовать негативное воздействие угроз информационной безопасности различной физической природы и функционального назначения без задействования самих объектов.

Особенности реализации экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов

Результаты проведенного анализа позволили выявить противоречие между необходимостью гарантированной защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем от угроз информационной безопасности, с одной стороны; и неспособностью существующих систем и средств обеспечить их эффективную защиту из-за отсутствия соответствующего математического, алгоритмического и программного обеспечения, с другой стороны.

Данное противоречие возможно разрешить путем теоретической разработки и практической реализации экосистемы информационной

безопасности на основе использования интеллектуальных цифровых двойников элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем. При этом, как показали проведенные исследования, существующие модели, методы и средства не способны обеспечить гарантированную защиту этих объектов от угроз информационной безопасности.

Создание экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов подразумевает разработку соответствующих моделей и методов создания и применения, а также алгоритмов и программных средств ее реализации, обеспечивающих гарантированную защиту элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем от угроз информационной безопасности.

Особенностями реализации такой экосистемы являются:

– формулирование принципов создания, архитектуры и модели организации, алгоритмов взаимодействия элементов экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов;

– наличие моделей обеспечения защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем на основе использования их интеллектуальных цифровых двойников;

– обоснование методов обеспечения защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем на основе использования их интеллектуальных цифровых двойников;

– реализация совокупности взаимодействующих в рамках единой цифровой платформы средств обеспечения защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем на основе использования их интеллектуальных цифровых двойников.

Заключение

Таким образом, проведен краткий анализ мер информационной безопасности, позволивший обосновать ведущую роль в современных условиях технических мер защиты элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем.

Результаты проведенного анализа роста показателей кибепреступности в России позволили выявить моральную устарелость существующего комплексного подхода к защите элементов компьютерных систем, цифровых систем, систем сотовой связи, а также пользователей этих систем, и определил необходимость, своевременность и актуальность создания и применения экосистемы информационной безопасности.

Результаты анализа существующих единичных решений по созданию и применению экосистем информационной безопасности позволили выявить необходимость применения интеллектуальных цифровых двойников защищаемых объектов для нейтрализации угроз информационной безопасности.

Определены особенности реализации экосистемы информационной безопасности на основе использования интеллектуальных цифровых двойников защищаемых объектов.

Литература

1. Бирюков А.А. Информационная безопасность: защита и нападение. 3-е изд., перераб. и доп. М.: ДМК Пресс, 2023. 440 с.

2. Обзор инструментов информационной безопасности // URL: sky.pro/wiki/profession/obzor-instrumentov-kiberbezopasnosti/.

3. 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.

4. Pollard, B., HTTP/2 in Action. Manning Publications. 2019. pp. 3–5. URL: dl.ebooksworld.ir/motoman/Manning.HTTP2.in.Action.EBooksWorld.ir.pdf

5. 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.

6. Flach, P.A., 2012. Machine Learning: The Art and Science of Algorithms that Make Sense of Data. Cambridge University Press, pp. 13–18. URL: cs.put.poznan.pl/tpawlak/files/ZMIO/W02.pdf.

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

8. 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.

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

10. BI.ZONE – компания по управлению цифровыми рисками // URL: bi.zone/?ysclid=mgav580h4j530700515.

11. R-Vision – разработчик надежных систем цифровизации и кибербезопасности// URL: rvision.ru/.

12. Защитные решения кибербезопасности для дома и бизнеса | Лаборатория Касперского // URL: kaspersky.ru/.

13. Газинформсервис – информационная безопасность // URL: gaz-is.ru/.

14. Anti-Malware.ru // URL: anti-malware.ru/analytics/Technology_Analysis/Cyber-Security%20Ecosystems.

References

1. Biryukov A.A. Informatsionnaya bezopasnost: zashchita i napadenie [Information security: defense and attack]. 3-e izd., pererab. i dop. M.: DMK Press, 2023. 440 p.

2. Obzor instrumentov informatsionnoi bezopasnosti // URL: sky.pro/wiki/profession/obzor-instrumentov-kiberbezopasnosti/.

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

4. Pollard, B., HTTP/2 in Action. Manning Publications. 2019. pp. 3–5. URL: dl.ebooksworld.ir/motoman/Manning.HTTP2.in.Action.EBooksWorld.ir.pdf

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

6. Flach, P.A., Machine Learning: The Art and Science of Algorithms that Make Sense of Data. Cambridge University Press. 2012. pp. 13–18. URL: cs.put.poznan.pl/tpawlak/files/ZMIO/W02.pdf.

7. Kiberprestupnost v Rossii: 765 tisyach sluchaev za 2024 god // URL: itsec.ru/news/kiberprestupnost-v-rossii-765-tisiach-sluchayev-za-2024-god.

8. Skolko kiberprestuplenii zafiksirovano v Rossii v 2025 godu i kakoi ot nikh ushcherb? – 18 iyunya 2025 | FONTANKA.ru // URL: fontanka.ru/2025/06/18/75604451/?ysclid=mgalbc1qnf500542194.

9. Kiberpoteri rossiiskoi ekonomiki – Mediaplatforma MirTesen // URL: nayavu.mirtesen.ru/blog/ 43689945896/ Kiberpoteri-rossiyskoy-ekonomiki.

10. BI.ZONE – kompaniya po upravleniyu tsifrovimi riskami // URL: bi.zone/?ysclid=mgav580h4j530700515.

11. R-Vision – razrabotchik nadezhnikh sistem tsifrovizatsii i kiberbezopasnosti // URL: rvision.ru/.

12. Zashchitnie resheniya kiberbezopasnosti dlya doma i biznesa | Laboratoriya Kasperskogo // URL: kaspersky.ru/.

13. Gazinformservis – informatsionnaya bezopasnost // URL: gaz-is.ru/.

14 Anti-Malware.ru // URL: anti-malware.ru/analytics/Technology_Analysis/Cyber-Security%20Ecosystems.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 15.09.2025

Дата публикации: 20.10.2025