Инженерный вестник Дона, №1 (2026)
ivdon.ru/ru/magazine/archive/n1y2026/10648

Исследование принципов построения и основных элементов экосистем информационной безопасности

Д.С. Горин, Р.Р. Шатовкин

МИРЭА – Российский технологический университет, Москва

Аннотация: В статье рассмотрены механизм создания экосистемы информационной безопасности и модели ее организации, а также проведен анализ требований к обеспечению защиты информации, функциональных областей обеспечения защиты информации и правил построения экосистем информационной безопасности. На основе проведенного анализа сформулированы основные принципы построения экосистем информационной безопасности, включающие: принципы разработки архитектуры экосистемы, принципы организации защиты объектов, принцип применения технологий и принципы реализации управления. Проведен анализ основных элементов экосистемы информационной безопасности. Исходя из традиционного представления, обусловленного ответным воздействием на угрозу, определен функционал элементов типовой экосистемы информационной безопасности. Обозначен альтернативный вариант построения экосистемы информационной безопасности на основе определения состава и функционального назначения ее элементов с учетом назначения, особенностей функционирования и характерных уязвимостей самих защищаемых объектов.
Ключевые слова: информационная безопасность, экосистема, принципы построения, стандарт, фреймворк кибербезопасности, средства информационной безопасности.

Введение

Создание и развитие экосистем информационной безопасности в настоящее время обусловлено не столько появившимися технологическими возможностями, сколько современными реалиями – в условиях постоянного роста интенсивности и совершенствования кибератак компании нуждаются в инновационных подходах к созданию и организации работы, в первую очередь, центров мониторинга информационной безопасности Security Operation Center (SOC) в интересах обеспечения эффективной защиты от угроз информационной безопасности.

Такой подход основан на решении ряда разноплановых задач информационной безопасности с помощью комплексной взаимосвязи различных технологий и средств их реализации в рамках единой платформы, что определило создание и развитие экосистем информационной безопасности.

Реализация экосистемы, в свою очередь, требует обоснования принципов ее построения, состава и архитектуры. Это требует всестороннего и глубокого анализа целей, особенностей и условий функционирования и применения экосистемы, а также ее элементов и процессов, происходящих в ней.

Цель статьи – исследование принципов построения экосистемы информационной безопасности и составляющих ее элементов.

Принципы построения экосистем информационной безопасности

Среди подходов к формированию экосистем, в целом, выделяют: проектный, стратегический, процессный, функциональный, радикальный, динамический [1].

Выбор конкретного подхода к формированию экосистемы зависит от выбранной стратегии, целей и масштаба применения.

Механизм создания экосистемы, в целом, без конкретизации области ее применения, проиллюстрирован на рис. 1 [2].

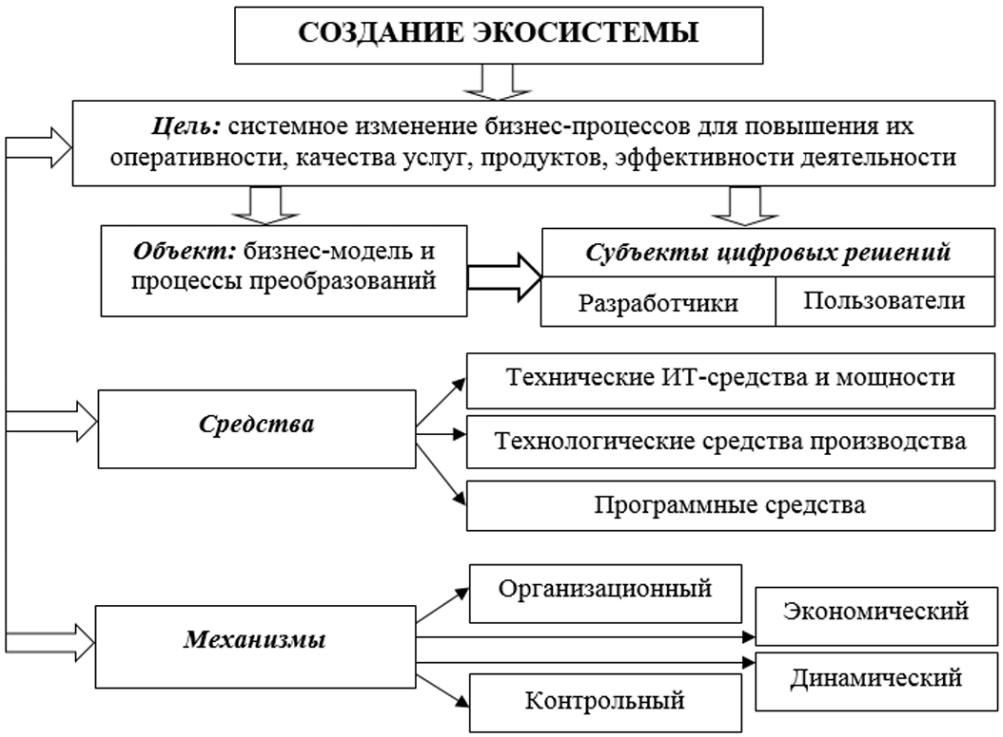

Рис. 1. – Механизм создания экосистемы

Данный механизм вполне применим и для создания экосистемы информационной безопасности.

В зависимости от публичности правил допуска выделяются закрытая, открытая и гибридная модели организации экосистемы (рис. 2) [3].

Рис. 2. – Модели организации экосистемы

При открытой модели организации экосистемы доступ к ней имеют конкурирующие поставщики услуг, их допуск осуществляется на основе публично раскрываемых правил.

При закрытой модели организации экосистемы правила доступа к ней публично не объявляются, а в роли поставщика услуг выступает сама экосистема, аффилированные с ней лица или ограниченный круг компаний-партнеров.

Гибридная модель сочетает как открытые, так и закрытые сегменты.

Для создания экосистемы информационной безопасности с учетом области ее применения наиболее целесообразным является использование закрытой модели.

Создание экосистемы информационной безопасности должно быть, в первую очередь, основано на принципах обеспечения защиты информации.

Так, в международном стандарте по информационной безопасности от 2005 года ISO/IEC 27001 «Information Technologies. Protection Methods. Information Security Management Systems. Requirements and Definitions» сформулированы следующие основные принципы обеспечения защиты информации:

– конфиденциальность – данные доступны только тем, кому они предназначены;

– целостность – данные остаются точными и не изменяются без разрешения владельца;

– доступность – данные получит именно тот, кому они нужны.

До определенного момента эти принципы полностью удовлетворяли практическим потребностям и определяли концепцию защиты информации.

Однако, с развитием облачных технологий и цифровой трансформацией уязвимость защищаемых данных многократно возросла [4].

В результате, распространение получили управляемые сервисы безопасности, вынуждающие пользователей полагаться на поставщиков услуг, как на часть своей экосистемы. Акцент при этом делался на сотрудничестве, обмене данными и их интеграции [5, 6].

В 2014 году государственным институтом стандартов и технологий США – National Institute of Standards and Technology Cybersecurity Framework (NIST) был разработан фреймворк Cybersecurity Framework Version 1.1, содержащий инструкции по оценке и повышению защищенности данных [7, 8].

Ядро фреймворка определяет 5 функциональных областей обеспечения информационной безопасности (рис. 3) [8]:

– идентификация (identify) – понимание рисков и знание активов организации;

– защита (protect) – реализация мер для предотвращения несанкционированного доступа и минимизации ущерба;

– обнаружение (detect) – мониторинг и выявление событий, связанных с кибератаками;

– реагирование (respond) – планирование и выполнение мероприятий по действиям в момент инцидента и после него;

– восстановление (recover) – перезапуск работы организации.

Рис. 3. – Функциональные области обеспечения защиты информации фреймворка кибербезопасности NIST

Помимо этого, в документе выделяется 4 уровня обеспечения защиты информации:

– частичный (partial): организация имеет ограниченное представление о рисках и слабую координацию мер безопасности;

– информированный о риске (risk informed): процессы управления рисками начинают формироваться, но еще не полностью интегрированы;

– повторяемый (repeatable): управление рисками становится обычной частью протекающих в системе процессов;

– адаптивный (adaptive): высокая интеграция процессов управления рисками.

Однако, главные правила построения экосистем информационной безопасности были сформулированы в работе «Enabling Distributed Security in Cyberspace» [9]:

1. Автоматизация процессов в экосистемах информационной безопасности приближает скорость реагирования на инцидент к скорости кибератаки.

2. Взаимодействие элементов экосистемы информационной безопасности позволяет решать соответствующие задачи с помощью политик, а не только технических ограничений.

Развитие методов построения интеллектуальных систем и методов искусственного интеллекта позволяет улучшить процессы взаимодействия между отдельными элементами экосистемы и, как следствие, повысить эффективность защиты объектов от угроз информационной безопасности.

3. Аутентификация гарантирует, что удаленные ресурсы и сторонние участники, с которыми осуществляется взаимодействие, являются подлинными.

Таким образом, процесс формирования и развития принципов построения экосистем информационной безопасности является ответной реакцией на появление новых и совершенствование существующих видов угроз.

На сегодняшний день при построении экосистемы информационной безопасности учитываются:

– требования: конфиденциальности, целостности и доступности информации (стандарт 27001);

– функциональные области обеспечения защиты информации: идентификация (identify); защита (protect); обнаружение (detect); реагирование (respond); восстановление (recover), а также уровни защиты информации: частичный (partial); информированный о риске (risk informed); повторяемый (repeatable); адаптивный (adaptive) (фреймворк NIST);

– правила построения экосистем информационной безопасности: автоматизация, взаимодействие и аутентификация («Enabling Distributed Security in Cyberspace»).

С учетом механизма создания, закрытой модели организации, требований к обеспечению защиты информации, функциональных областей обеспечения

защиты информации и правил построения экосистем информационной безопасности возможно сформулировать основные принципы их построения. Они включают принципы разработки архитектуры экосистемы, организации защиты объектов, применения технологий и реализации управления.

К принципам разработки архитектуры экосистемы правомерно отнести:

– принцип реализации многоуровневой защиты – средства защиты в составе экосистемы применяются на разных уровнях, обеспечивая эшелонированную защиту объектов от угроз информационной безопасности;

– принцип адаптируемости – экосистема должна учитывать динамику развития угроз информационной безопасности, обеспечивая превентивные меры защиты объектов от угроз информационной безопасности;

– принцип масштабируемости – экосистема должна учитывать количественный рост и интенсивность воздействия угроз, обеспечивая гарантированную защиту объектов от угроз информационной безопасности;

– принцип высокой интеграции элементов – экосистема должна обеспечивать взаимовыгодное взаимодействие составляющих ее элементов в интересах достижения ими общей цели – эффективной защиты объектов от угроз информационной безопасности;

– принцип удобства применения и простоты контроля – экосистема должна быть удобна в эксплуатации, не требовать сложных настроек и проста для диагностики.

Принципы организации защиты объектов в экосистеме:

– принцип представления информационной безопасности в виде непрерывного процесса – информационная безопасность не заканчивается на моменте внедрения экосистемы, а продолжается на протяжении всего жизненного цикла защищаемого объекта;

– принцип «никому не доверять, всегда проверять» – отражает необходимость верификации пользователей, устройств и приложений на

каждом этапе их взаимодействия с применением средств постоянного анализа угроз и адаптации политик безопасности.

Принципом применения технологий в экосистеме является принцип непрерывной интеграции новых технологий и решений в существующие инфраструктуры.

Принципы реализации управления в экосистеме:

– принцип единой платформы взаимодействия элементов экосистемы – обеспечивает оперативность, непрерывность и гибкость управления элементами экосистемы информационной безопасности;

– принцип воспитания культуры безопасности – регулярное обучение пользователей вопросам информационной безопасности.

Обозначенные принципы направлены на минимизацию рисков утечек данных и последствий воздействия угроз информационной безопасности.

Основные элементы экосистем информационной безопасности

Существуют различные подходы к определению состава и назначения элементов экосистем информационной безопасности. Они достаточно подробно описаны в работах [6, 10].

Рассмотрим состав экосистемы информационной безопасности [11–13]:

1. Антивирусное программное обеспечение: 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.

2. Межсетевые экраны (аппаратные, программные): контролируют сетевой трафик на основе заданных правил безопасности; играют ключевую роль в защите сетей от несанкционированного доступа и предотвращают распространение вредоносных программ.

3. Системы обнаружения и предотвращения вторжений – Intrusion Detection System / Intrusion Prevention System (IDS / IPS): мониторят сетевой трафик на предмет подозрительной активности и автоматически блокируют потенциальные угрозы; IDS обнаруживает подозрительную активность и уведомляет администратора; IPS автоматически блокирует угрозы.

4. Виртуальные частные сети – Virtual Private Network (VPN): защищают информацию в открытой сети путем шифрования трафика.

5. Криптографические средства: защищают данные за счет их шифрования при передаче и хранении.

6. Системы управления идентификацией и доступом – Identity and Access Management (IAM): позволяют настраивать доступ и осуществлять контроль над работой с данными.

7. Системы многофакторной аутентификации: за счет применения ряда способов удостоверения личности создают повышенный уровень безопасности.

8. Тестирование на проникновение (пен-тесты): имитируют угрозы, что позволяет выявить слабые места системы безопасности.

9. Средства статического и динамического анализа кода: анализируют исходный код приложений на предмет уязвимостей, таких как Structured Query Language (SQL)-инъекции или межсайтовый скриптинг – Cross-Site Scripting (XSS); 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.

10. Системы управления событиями и данными безопасности – Security Information and Event Management (SIEM)-системы: собирают и производят анализ данных из различных источников для выявления корреляции событий; позволяют своевременно реагировать на возникающие инциденты информационной безопасности.

11. Системы автоматизации и оркестровки – Security Orchestration, Automation and Response (SOAR): координируют работу средств защиты и ускоряют реагирование на угрозы.

12. Системы обнаружения и реагирования на инциденты в конечных точках – Endpoint Detection and Response (EDR): производят сканирование на угрозы, осуществляют проверку уязвимостей, автоматически анализируют инциденты и осуществляют быстрое реагирование на них.

13. Инструменты технологии расширенного обнаружения угроз и реагирования на них – Extended Detection and Response (XDR)-решения: расширяют возможности EDR, охватывая не только конечные устройства, но и корпоративные сети, и другие ресурсы.

14. Средства защиты от Distributed Denial of Service (DDoS)-атак: предназначены для борьбы с распределенными атаками, направленными на перегрузку серверов, приложений и сетей.

15. Средства резервирования: позволяют создавать резервные копии данных.

Обозначенные инструменты и решения формируют многогранную экосистему информационной безопасности, позволяющую организациям обеспечить защиту информации от различных угроз. Однако, функционал обозначенных средств и систем определяется, исходя из традиционного представления, обусловленного ответным воздействием на угрозу.

Такое положение определяет наследование части недостатков, присущих комплексному применению отдельных систем и средств защиты вне единой платформы, и их роли «догоняющего», что не обеспечивает превентивности мер защиты. В этом случае альтернативным вариантом, подлежащим дальнейшему исследованию, может быть определение состава и функционального назначения элементов экосистемы информационной безопасности с учетом назначения, особенностей функционирования и

характерных уязвимостей защищаемых объектов. Как следствие, роль «догоняющего» в развитии средств обеспечения информационной безопасности изменится на роль «обороняющего» защищаемый объект вне зависимости от вида угрозы.

Заключение

Таким образом, рассмотрены механизм создания экосистемы информационной безопасности и модели ее организации, а также проведен анализ требований к обеспечению защиты информации, функциональных областей обеспечения защиты информации и правил построения экосистем информационной безопасности.

На основе проведенного анализа сформулированы основные принципы построения экосистем информационной безопасности, включающие: принципы разработки архитектуры экосистемы, принципы организации защиты объектов, принцип применения технологий и принципы реализации управления.

Проведен анализ основных элементов экосистемы информационной безопасности. Установлено, что функционал элементов типовой экосистемы информационной безопасности в настоящий момент определяется, исходя из традиционного представления, обусловленного ответным воздействием на угрозу. Это определяет наследование части недостатков, присущих комплексному применению отдельных систем и средств защиты вне единой платформы, и их роли «догоняющего», что не обеспечивает превентивности мер защиты.

Альтернативным вариантом построения экосистемы информационной безопасности в этом случае является определение состава и функционального назначения ее элементов с учетом назначения, особенностей функционирования и характерных уязвимостей самих защищаемых объектов.

Литература

1. Бабкин А.В., Алетдинова А.А., Буркальцева Д. Д., Батукова Л. Р. Бухвальд Е. М Григорьева Е. Э. Гилева Т.А., Герасимов В.И., Гончаренко Т.В, Damary R.G.C., El Hallak A., Егоров Н.Е., Alon I., Клачек П.М., Либерман И.В, Лычагин М.В, Марковская Е.И, Махмудова Г.Н., Милёхина О.В., Нехорошева Л.Н., Osińska M., Sabri. O., Schuur P., Степанов Е.А., Устинова Л.Н., Тинякова В.И., Шамина Л.К., Шкарупета Е.В. Экосистемы в цифровой экономике: драйверы устойчивого развития: монография // СПб: Политех-Пресс, 2021. 778 с.

2. Шаравова О.И., Кузовков А. Д., Шаравова М.М. Концепции, модели и принципы построения экосистем в условиях сетевой экономики // Электронный научный журнал «Век качества». 2025. № 1. С. 105–130. URL: agequal.ru/pdf/2025/125007.pdf.

3. Банк России. Экосистемы: подходы к регулированию. Доклад для общественных консультаций. М.: Центральный банк Российской Федерации, 2021. 46 с. URL: library.cbr.ru/catalog/lib/books/390835/.

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

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

6. Как устроены экосистемы кибербезопасности и зачем они нужны заказчикам // URL: anti-malware.ru/analytics/Technology_Analysis/Cyber-Security-Ecosystems-do-we-need-them.

7. Getting Started with CSF 1.1 | NIST // URL: nist.gov/cyberframework/getting-started-csf-11.

8. NIST Releases Version 1.1 of its Popular Cybersecurity Framework | NIST // URL: nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

9. Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. U.S. Department of Homeland Security. 2011. 29 p. URL: dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

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

11. 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.

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

13. 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.

References

1. Babkin A.V. Ekosistemi v tsifrovoi ekonomike: draiveri ustoichivogo razvitiya: monografiya [Ecosystems in the Digital Economy: Drivers of Sustainable Development: monograph]. Aletdinova A.A., Burkal'ceva D. D., Batukova L. R. Buhval'd E. M Grigor'eva E. E. Gileva T.A., Gerasimov V.I., Goncharenko T.V, Damary R.G.C., El Hallak A., Egorov N.E., Alon I., Klachek P.M., Liberman I.V, Lychagin M.V, Markovskaya E.I, Mahmudova G.N., Milyohina O.V., Nekhorosheva L.N., Osińska M., Sabri. O., Schuur P., Stepanov E.A., Ustinova L.N., Tinyakova V.I., SHamina L.K., SHkarupeta E.V. SPb.: Politekh-Press, 2021. 778 p.

2. Sharavova O.I., Kuzovkov A. D., Sharavova M.M. Kontseptsii, modeli i

printsipi postroeniya ekosistem v usloviyakh setevoi ekonomiki. [Concepts, models, and principles of ecosystem building in a networked economy] Elektronnii nauchnii zhurnal «Vek kachestva». 2025. № 1. Pp. 105–130. URL: agequal.ru/pdf/2025/125007.pdf.

3. Bank Rossii. Ekosistemi: podkhodi k regulirovaniyu. Doklad dlya obshchestvennikh konsultatsii [Bank of Russia. Ecosystems: Approaches to Regulation. Report for Public Consultation]. M.: Tsentralnii bank Rossiiskoi Federatsii, 2021. 46 p. URL: library.cbr.ru/catalog/lib/books/390835/.

4. 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.

5. Arakhmeeva K.A., Vistunov S.S. Ekonomika i kachestvo sistem svyazi. 2024. № 3. Pp. 119–126.

6. Kak ustroeni ekosistemi kiberbezopasnosti i zachem oni nuzhni zakazchikam [How do cybersecurity ecosystems work and why do customers need them]. URL: anti-malware.ru/analytics/Technology_Analysis/Cyber-Security-Ecosystems-do-we-need-them.

7. Getting Started with CSF 1.1 | NIST. URL: nist.gov/cyberframework/getting-started-csf-11.

8. NIST Releases Version 1.1 of its Popular Cybersecurity Framework. NIST. URL: nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular- cybersecurity-framework.

9. Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. U.S. Department of Homeland Security. 2011. 29 p. URL: dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

10. 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.

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

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

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

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 15.10.2025

Дата публикации: 25.12.2025