СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЫНКА ЭКОСИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.А. Ахрамеева, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», ksenya_2002@mail.ru;*
С.С. Вистунов, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», solekvis@yandex.ru.*

УДК 004.056

Аннотация. В данной статье представлен результат сравнительного анализа рынка готовых решений для внедрения экосистем информационной безопасности в разрезе крупного и среднего бизнеса. Определены преимущества и недостатки сравниваемых компаний, предоставляющих услуги развертывания экосистем информационной безопасности.

Ключевые слова: экосистема ИБ; защита; информация; информационная безопасность; технологии.

COMPARATIVE ANALYSIS OF THE INFORMATION SECURITY ECOSYSTEM MARKET

Kseniia Akhrameeva, *Ph.D. of Engineering Sciences, Associate Professor, The Bonch-Bruevich Saint Petersburg State University of telecommunications;*
Stepan Vistunov, *The Bonch-Bruevich Saint Petersburg State University of telecommunications.*

Annotation. This article presents the results of a comparative analysis of the market of ready-made solutions for the implementing for the information security ecosystems in large and medium-sized businesses. The advantages and disadvantages of the compared companies providing information security ecosystem deployment services are identified.

Keywords**:** information security ecosystem; protection; information; information security; technology.

Введение

В связи с активным развитием технологий информационной безопасности (ИБ) в современном мире, а также методов кибератак, для каждой компании немаловажным является правильный выбор поставщика защитного программного обеспечения, которое сформирует экосистему ИБ предприятия. Целью данной статьи является изучение рынка готовых решений для создания экосистем информационной безопасности, а также проведение сравнительного анализа компаний, предоставляющих такие решения.

Сравнительный анализ экосистем

Как правило, на рынке экосистемы информационные технологии представлены в виде продукта или наборов продуктов, которые поставляет некая компания-поставщик *(vendor)*. Такие фирмы могут иметь готовые решения для потребности компании в данный момент или же создавать конкретные решения по запросу

компании-потребителя, которые будут предоставлены в виде локальной, облачной или гибридной модели экосистемы [1].

Большая часть компаний, которые предоставляют подобные услуги, реализуют свои решения с помощью облачной или гибридной модели экосистемы ИБ. Это связано с тем, что готовые решения уже развернуты на их серверах, а все, что остается сделать, это подключить к своей сети компанию-потребителя, однако такие фирмы могут предоставить для компании решение, которое ей необходимо, с реализацией локальной экосистемы. Основная проблема такого подхода заключается в том, что в случае, если компания-потребитель будет подвержена кибератаке, компания с локальной экосистемой будет в одиночку решать проблемы, последующие за атакой. А компания-поставщик отвечает только за установку оборудования и предоставление решения по безопасности. Также на компанию-потребителя возлагаются большие разовые затраты, которые будут включать в себя оплату оборудования и наем специалистов для работы в собственной инфраструктуре [6].

В случае если компания-поставщик предоставляет услуги типа *MSSP* (*Managed Security Service Providers*) или же *SECaaS* (*Security-as-a-Service*), означающие, что фирма предоставляет услуги безопасности как сервиса, то чаще придерживаются облачной или гибридной модели экосистем [1].

Разберем примеры предоставляемых услуг некоторых компаний, которые занимаются развертыванием экосистем информационной безопасности.

Компания «*BI.ZONE*». Сама компания имеет слоган *BI.ZONE*: «Комплексная кибербезопасность для вашего бизнеса». В основе концепции *BI.ZONE* лежит комплексный подход к обеспечению кибербезопасности и непрерывности бизнеса [2].

Компания предлагает набор практик и инструментов, позволяющих:

- повысить киберустойчивость компании в условиях постоянно меняющихся угроз;
- создать собственный центр кибербезопасности (*SOC*);
- использовать центр мониторинга по модели *SecaaS*;
- оснастить центр кибербезопасности компании.

BI.ZONE предлагает широкий спектр продуктов и услуг:

- средства для пентестинга (*BI.ZONE CPT*);
- платформа *BI.ZONE Bug Bounty* для запуска программ вознаграждения за найденные уязвимости;
- *BI.ZONE Secure DNS* для защиты бизнеса от атак с использованием *DNS*;
- *BI.ZONE Brand Protection* для защиты бренда;
- *BI.ZONE TDR Threat Detection and Response* – решение для непрерывного мониторинга безопасности;
- платформа для сбора, верификации и распространения потоков данных *Threat Intelligence*;
- служба получения сведений об актуальных киберугрозах *BI.ZONE ThreatVision*;
- *BI.ZONE Secure SD-WAN* – сервис для безопасной трансформации сети;
- *BI.ZONE AntiFraud* (*BI.ZONE BFP*) – средство противодействия мошенничеству;
- услуги по реагированию на инциденты;
- *BI.ZONE Compromise Assessment* – проверка всей инфраструктуры на предмет компрометации;
- приватное облако *BI.ZONE* для безопасного взаимодействия с внешним миром;
- *WAF* и защита электронной почты.

BI.ZONE работает по сервисной модели и специализируется на аутсорсинге.
Компания предлагает следующие услуги:

- функции сервис-провайдера;
- экспертные услуги и консалтинг;
- широкую линейку инструментов кибербезопасности;
- *BI.ZONE Compliance Platform* – решение для построения зрелых процессов, необходимых для соответствия требованиям федерального закона № 152-ФЗ;
- сервис «Виртуальный директор по кибербезопасности» (*BI.ZONE vCISO*).

Преимуществом компании является комплексный подход к индивидуальным стратегическим проектам в области кибербезопасности. Этот подход включает в себя несколько последовательных этапов, таких как аудит защиты, разработка архитектуры кибербезопасности, тестирование сервисов, аудит технической инфраструктуры, внедрение сервисов кибербезопасности, а также их сопровождение и поддержка. Заказчики, уже имеющие сформированные собственные команды по кибербезопасности, особенно заинтересованы в блоке решений по управлению уязвимостями, вознаграждениям за нахождение уязвимостей (баг-баунти) и использовании киберполигона.

Недостатками компании является то, что *BI.ZONE*, в основном, фокусируется на собственных продуктах и решениях, что может ограничить возможности интеграции с другими экосистемами ИБ, а также предоставляет неполный набор функций для управления экосистемой ИБ, что может потребовать использования дополнительных решений от других поставщиков.

Компания *R-Vision EVO* [4]. *R-Vision EVO* представляет собой экосистему взаимосвязанных технологий, компонентов и процессов, предназначенных для построения и развития *SOC* (*Security Operations Center*).

Создание экосистемы *R-Vision EVO* стало логичным продолжением многолетней работы компании по разработке продуктов для *SOC* [4].

Основная задача *R-Vision EVO*:

- предоставить компаниям возможность поэтапного развития *SOC*, его технологий и процессов;
- обеспечить комплексную кибербезопасность организации.

R-Vision использует лучшие практики риск-ориентированного подхода:

- инвентаризация активов;
- оценка рисков;
- мониторинг инфраструктуры;
- выявление инцидентов;
- реагирование на инциденты.

Все эти процессы непрерывны и позволяют эволюционно развивать *SOC*.
Внедрение технологий *R-Vision EVO*:

- расширяет возможности детектирования;
- обеспечивает дополнительный контекст при расследовании инцидентов;
- помогает избежать финансовых и репутационных потерь;

Построение эффективного *SOC* на базе *R-Vision EVO:*

- *Security Asset Management*: Формирование полной видимости инфраструктуры, оценка активов и их критической значимости.

- *Governance, Risk Management, Compliance*: Работа с рисками, оценка состояния защиты, определение вероятности реализации угроз и возможного ущерба.
- *Vulnerability Management*: Автоматизация работы с уязвимостями, их выявление, приоритизация и устранение.
- *Security Information and Event Management*: Мониторинг инфраструктуры, сбор событий со всех активов, их нормализация, хранение и анализ.
- *Security Orchestration, Automation and Response*: Автоматизация управления инцидентами в ИБ за счет преднастроенных сценариев.
- *User and Entity Behavior Analytics*: Детальное расследование инцидентов, обнаружение отклонений от нормального поведения пользователей и объектов;
- *Deception*: Имитация элементов инфраструктуры для обнаружения злоумышленников и замедления их передвижения в сети.
- *Threat Intelligence*: Всестороннее управление данными о киберугрозах.

Использование экосистемы кибербезопасности *R-Vision EVO* при создании *Security Operations Center* (*SOC*) предоставляет ряд преимуществ. Эта экосистема позволяет поэтапно расширять функциональность *SOC* в соответствии с потребностями организации, обеспечивая адаптацию к изменяющимся угрозам. Встроенные интеграционные механизмы, конфигурации и ролевые модели экосистемы упрощают процесс интеграции компонентов и обеспечивают единое управление и контроль над всеми технологиями *SOC*. [8] Компания *R-Vision* предлагает экосистемный подход, который помогает разрабатывать долгосрочные планы развития *SOC* и эффективно защищать организацию, предоставляя инструменты и ресурсы для планирования и управления развитием *SOC* с учетом специфических задач заказчика. Кроме того, вендор обеспечивает экспертную поддержку внедрения технологий *R-Vision EVO*, включая консультации, обучение персонала, настройку системы и постоянное сопровождение в процессе эксплуатации *SOC*. Цель развития экосистемы *R-Vision EVO* заключается в предоставлении заказчику уникального набора технологий, которые помогут создать долгосрочные планы развития *SOC* и будут полезны на всех этапах его развития.

Компания «Лаборатории Касперского» [3]. Экосистема информационной безопасности «Лаборатории Касперского» разработана компанией для активной борьбы за рынок экосистем ИБ. Она начала свое развитие с отдельных продуктов и постепенно перешла к комплексным решениям, объединяющим несколько систем информационной безопасности (ИБ-систем). В конце 2021 г. компания представила решение под названием *Kaspersky Symphony XDR*, которое является ключевым элементом экосистемы. *Symphony XDR* обладает технологиями автоматического предотвращения, мониторинга, обнаружения, расследования, проактивного поиска, анализа первопричин и предотвращения атак. Оно предназначено для компаний всех размеров и отраслей, но особенно актуально для крупных организаций, где высокие требования к безопасности и есть специалисты, работающие с передовыми решениями.

«Лаборатория Касперского» считает, что комплексный подход и экосистема информационной безопасности не являются одним и тем же. Экосистема должна включать все необходимое для борьбы с современными атаками и, в первую очередь, предназначена для крупных компаний, таких как промышленные организации и финансовые учреждения. Вендор предлагает экосистемы, учитывающие специфику различных отраслей, и в 2022 г. представил *Kaspersky OT CyberSecurity*, которая ориентирована на промышленные предприятия [3]. Она включает в себя

специализированную промышленную *XDR*-платформу *Kaspersky Industrial CyberSecurity* и интегрируется с экосистемой для корпоративного сегмента.

Экосистема «Лаборатории Касперского» предоставляет ряд преимуществ. Она позволяет заказчику сократить издержки, благодаря единому лицензированию, поддержке и управлению компонентами, а также обеспечивает доступ к передовой аналитике по угрозам. Технологически экосистема строится на централизации и автоматизации. Автоматизация сокращает трудозатраты аналитиков на типичные операции, снижает выгорание специалистов и устраняет человеческие ошибки. Централизация позволяет собирать и анализировать инциденты со всех интегрированных продуктов, обеспечивая фокусировку на значимых угрозах.

«Лаборатория Касперского» утверждает, что их экосистема информационной безопасности является не просто концепцией, а реальной потребностью, которая делает процессы обеспечения безопасности более стабильными, эффективными и прозрачными. Она предоставляет ИБ-командам продвинутые инструменты и технологии для борьбы с угрозами любого масштаба и сложности, не перегружая специалистов. В результате система безопасности становится целостной, гибкой и адаптивной к изменяющейся угрозой среде. Экосистема информационной безопасности «Лаборатории Касперского» стремится обеспечить комплексную защиту организаций, улучшить проективное обнаружение и реагирование на инциденты, а также повысить эффективность работы ИБ-специалистов.

Компания «Газинформсервис» [5]. «Газинформсервис» (ГИС) – это компания, предоставляющая комплексные решения в сфере ИБ. ГИС предлагает клиенту широкий спектр продуктов и услуг, в которые входят: средства защиты информации, услуги по аудиту и консалтингу, а также предлагает интеграцию готовых решений для экосистем ИБ. Это позволяет заказчику обеспечить комплексную защиту *IT*-инфраструктуры, при этом не обязательно переходить только на продукты компании ГИС, а возможно объединить в единый защитный комплекс применяемые программные продукты других компаний и продукты ГИС.

Продукты компании ГИС закрывают такие области, как:

- защита *ИТ*-инфраструктуры – линейка продуктов *Efros* (комплекс программных и программно-аппаратных средств, предназначенный для защиты информации от несанкционированного доступа, модификации, уничтожения, кражи и других угроз) [7];
- защита рабочих станций и серверов – *SafeNode* (программно-техническое средство, встраиваемое в *UEFI BIOS*, обеспечивающее защиту от несанкционированного доступа к рабочим станциям и серверам с момента их включения до момента старта операционной системы) [7] и Блокхост-сеть (средство контроля съемных машинных носителей информации, управления двухфакторной аутентификацией и защиты от несанкционированного доступа ресурсов рабочих станций и серверов);
- электронный документооборот – *Litoria* (создание внешнего и внутреннего юридически значимого электронного документооборота);
- защита *SAP* – *SafeERP* (многофункциональный модульный комплекс по защите бизнес-приложений *SafeERP* обеспечивает контроль безопасности *ERP* систем, размещенных на платформах *1С* и *SAP*);
- информационные системы – *СУБД Jatoba* (ПО общего назначения, предназначенное для создания и управления реляционными базами данных. *СУБД Jatoba* обеспечивает многопользовательский доступ к расположенным в ней данным с разным уровнем конфиденциальности) [10];

- управление *ИБ* – *Ankey ASAP* (Платформа расширенной аналитики безопасности с функциями поведенческого анализа на базе *ИИ*), *Ankey IDM* (Программный продукт для централизованного управления учетными записями пользователей и их полномочиями в корпоративных информационных системах, включающий лучшие решения *IGA* (*Identity Governance and Administration*)), *Ankey SIEM* (Система мониторинга событий информационной безопасности и выявления инцидентов в реальном времени) [9]. Обеспечивает комплексный мониторинг информационной безопасности как всей инфраструктуры организаций, так и отдельных подразделений, узлов и приложений. Система адаптируется практически к любой инфраструктуре и работает для всех уровней управления – от рядового администратора до руководителя предприятия).

Система управления информационной безопасностью «Газинформсервис» – это комплекс мер, направленных на обеспечение информационной безопасности организации. *СУИБ* «Газинформсервис» включает в себя разработку политик и процедур *ИБ*, аудит *ИБ*, обучение сотрудников по вопросам *ИБ* и другие мероприятия.

Материал выше предоставляет общее понимание, на каких задачах концентрируется та или иная фирма, с выводом об их преимуществах, что позволяет провести сравнительный анализ деятельности этих компаний (табл. 1).

Таблица 1.

Критерий	*BI.ZONE*	*R-VISION*	*Kaspersky*	ГИС
Фокус	Экспертиза, сервисная модель	Экосистемный подход, риск-ориентированный подход	Глобальный лидер, инновации	Готовые решения, интеграция экосистем
Продукты и услуги	Пентестинг, *Bug Bounty*, *SecaaS*, консалтинг	*EVO, SAM, EDR, Threat Intelligence*	Защита домашних пользователей, защита предприятий, *Threat Intelligence*	*Litoria, СЗИ “ Efros ”, SafeNode , Ankey ASAP, Ankey SIEM, Ankey IDM , СУБД Jatoba, SafeERP*
Подход к развитию *SOC*	Индивидуальный подход	Планомерное развитие	Разнообразные решения	Многоуровневая защита
Преимущества	Глубокая экспертиза, гибкость	Экосистемный подход, адаптивность	Глобальный охват, инновации	Широкий спектр продуктов и услуг, использование ИИ, интегрируемость
Недостатки	Относительно высокая стоимость	Требует квалифицированн ого персонала	Может быть сложно для небольших организаций	Относительно высокая стоимость услуг и продуктов

Каждая компания имеет свои особенности:

BI.ZONE:

- фокус на экспертизе: пентестинг, *Bug Bounty*, защита бренда;
- сервисная модель: *SecaaS*, экспертные услуги, консалтинг;

- индивидуальный подход: стратегические проекты, аудит, развертывание сервисов.

R-VISION:
- экосистемный подход: *EVO*, планомерное развитие *SOC*;
- риск-ориентированный подход: управление активами, оценка рисков;
- широкий спектр технологий: от *SAM* до *Threat Intelligence*.

Kaspersky:
- глобальный лидер: многолетний опыт, широкий охват рынка;
- широкий спектр продуктов: для всех типов организаций, от домашних пользователей до крупных предприятий;
- фокус на инновациях: машинное обучение, искусственный интеллект.

Газинформсервис
- комплексный подход к защите информации;
- интеграция рисков *ИБ* в существующую систему управления рисками;
- не требует строгого соответствия средств защиты информации одной экосистеме и работает с различными источниками.

Заключение

В данной статье проведен сравнительный анализ некоторых компаний, занимающихся предложением готовых решений или же создания необходимой экосистемы с учетом *IT*-инфраструктуры компании заказчика. Важно отметить, что не существует универсального решения для экосистемы по информационной безопасности и что лучшей экосистемой будет та, которая соответствует потребностям заказчика. При правильном подходе к выбору и реализации экосистемы можно значительно повысить уровень защиты организации от киберугроз. Важно учитывать, что не существует готового решения для каждой компании, а идеальной экосистемой информационной безопасности является экосистема, соответствующая всем требованиям компании заказчика.

Литература

1. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Security-Ecosystems (дата обращениея апрель 2024 г.).
2. URL: https://bi.zone/ (дата обращениея апрель 2024 г.).
3. URL: https://www.kaspersky.ru (дата обращениея апрель 2024 г.).
4. URL: https://www.rvision.ru/ (дата обращениея апрель 2024 г.).
5. URL: https://www.gaz-is.ru/ (дата обращениея апрель 2024 г.).
6. Волкогонов В.Н., Гельфанд А.М., Деревянко В.С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019), 2019. – С. 262-266.
7. Волкогонов В.Н., Гельфанд А.М., Карамова М.Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019), 2019. – С. 266-270.
8. Виткова Л.А. и др. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга //

Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018), 2018. – С. 140-142.
9. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации, 2021. – Т. 9. – С. 1-2.
10. Штеренберг С.И. Компьютерные вирусы. Часть 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.