УДК 338.46

АНАЛИЗ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Ионина М.В.
Санкт-Петербургский имени В.Б. Бобкова филиал Российской таможенной академии

ANALYSIS OF APPROACHES TO ENSURING INFORMATION SECURITY OF A COMPANY

Ionina M.V.
St. Petersburg named after V.B. Bobkov Branch of the Russian Customs Academy

Аннотация

В условиях цифровизации бизнес-процессов частных компаний и государственных структур, а также влияния масштабных кибератак последних лет и введения законодательных актов, регламентирующих задачи по импортозамещению в области критической информационной инфраструктуры, усиления наказания за утечку конфиденциальной информации, главной целью компаний становится обеспечение комплексной защиты информационной безопасности. Автором проведен анализ существующих подходов к организации информационной безопасности, необходимых для достижения данной цели.

Ключевые слова: цифровизация, информационная безопасность, провайдер, экосистема.

Abstract

In the context of the digitalization of business processes of private companies and government agencies, as well as the impact of large-scale cyber-attacks in recent years and the introduction of legislation regulating the tasks of import substitution in the field of critical information infrastructure, increasing penalties for the leakage of confidential information, the main goal of companies is to ensure comprehensive information protection security. The author analyzed existing approaches to organizing information security necessary to achieve this goal.

Keywords: digitalization, information security, provider, ecosystem.

Ссылка для цитирования: Ионина М.В. Анализ подходов к обеспечению информационной безопасности компании // Бюллетень инновационных технологий. – 2024. – Т. 8. – № 1(29). – С. 48-53. – EDN SLXTQI.

Масштабные кибератаки на фоне сложившейся геополитической обстановки последних лет наглядно показывают риски, связанные с утечкой конфиденциальных данных, нарушением работоспособности информационных систем и т.д., что безусловно стимулирует компании принимать решения, направленные на улучшение мер комплексной защиты информационной инфраструктуры. «Одной из таких крупных кибератак, имеющей резонансный характер, была атака, совершенная 10 апреля 2023 года на единую автоматизированную информационную систему таможенных органов (ЕАИС ТО), которая привела к мощнейшим сбоям в работе системы. Для восстановления ее полной работоспособности потребовалось продолжительное время: лишь 21 апреля временно исполняющий обязанности руководителя Федеральной таможенной службы России Р.В. Давыдов сообщил о полной ликвидации последствий случившейся проблемы» [1]. При деструктивных воздействиях на основные бизнес-процессы, ведущих к приостановке, либо к полной блокировке функционирования, компания вынужденно пересматривает текущий подход к организации информационной безопасности (ИБ). Лишь всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре, и является информационной безопасностью, задачи которой сводятся к

минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий [2, 3].

Согласно данным аналитиков Solar JSOC, специализированного отдела по анализу кибербезопасности в «компании «РТК-Солар», было реализовано приблизительно 80 проектов в различных отраслях, таких как государственный сектор, телекоммуникации, энергетика, информационные технологии и розничная торговля» [3]. Полученные данные позволяют предположить, что компании серьезно заботятся о безопасности своей информационно-технологической инфраструктуры. Это связано с систематическими кибератаками после начала СВО, активным использованием злоумышленниками различных уязвимостей и отчетами специалистов по ИБ о существующих угрозах. В частности, это касается корпоративных веб-приложений, которые всегда были и остаются наиболее уязвимым звеном внешнего периметра. Если в начале 2022 года низкий уровень защищенности таких приложений отмечался в 53% проектов, то теперь этот показатель снизился до 20% [4].

В 2023 году спрос на проведение киберучений в крупных российских компаниях увеличился приблизительно в два раза по сравнению с предыдущим годом. Услуга востребована прежде всего среди организаций из телекоммуникационной отрасли, а также сфер финансов и промышленности. Об этом говорится в исследовании ИТ-интегратора «Инфосистемы джет», результаты которого обнародованы 24 января 2024 года [5]. На спрос также повлиял законопроект об оборотных штрафах за утечку персональных данных, который Государственная Дума Российской Федерации приняла в первом чтении 23 января 2024 года [6].

Дополнительный объем задач в сфере кибербезопасности диктуют новые требования регуляторов. Самыми масштабными за последнее время стали требования Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [7]. Согласно закону, все ключевые предприятия страны, являясь субъектами критической информационной инфраструктуры (КИИ), должны выполнить ряд требований: провести категорирование, обеспечить безопасность объектов КИИ и осуществлять взаимодействие с ГосСОПКА (Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак). Большая часть требований направлена на выстраивание и обеспечение долгосрочных процессов ИБ. Речь идет о процессах мониторинга и выявления инцидентов ИБ [8].

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в январе 2024 года опубликовало Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием, согласно которым установлены сроки перехода на отечественный софт для госкомпаний:

– с 1 января 2025 года должны будут использоваться российские операционные системы (ОС), офисные пакеты, антивирусы.

– с января 2026 года планируют перейти на отечественные системы управления базами данных (СУБД) [10].

В отчете от 2023 года Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий сказано, что доля российского ПО в закупках госкомпаний составила 87,1% в количественном выражении и 54,2% в денежном [10].

По оценке участников рынка в сфере информационных технологий, основной трудностью остаются проблемы совместимости решений с текущим софтом и оборудованием. Учитывая возможные риски, которые могут возникнуть при реализации кибератак, и введенные нормативно-правовые акты, регламентирующие сферу ИБ, стимулируют как частные компании и государственные структуры к выстраиванию своей политики кибербезопасности, а также к созданию комплексной системы защиты от внешних и внутренних киберугроз. Наиболее распространенными услугами являются комплексные решения по защите от кибератак:

1. Провайдер (Managed Security Service Provider, (MSSP) – поставщик управляемых услуг безопасности, обеспечивает мониторинг и управление устройствами и системами безопасности компании [11].

2. Построение собственного центра мониторинга информационной безопасности (Security Operations Center, (SOC).

3. Развивающаяся в последние годы тенден¬¬ция на построение и развитие экосистемы ИБ.

В каждом из решений в рамках комплексной защиты архитектуры информационной безопасности компании от киберугроз существуют свои плюсы и минусы, а

также принципиальные отличия, которые проявляются как в подходах к реализации данных решений, так и в комплексе продуктов и услуг, направленных на защиту ИБ, и зависят от потребностей и стратегии безопасности конкретной организации.

1. Провайдер управляемых услуг безопасности (MSSP) обеспечивает внешний мониторинг и управление устройствами и системами безопасности. Общие услуги включают управляемый межсетевой экран, обнаружение вторжений, виртуальную частную сеть, сканирование уязвимостей и антивирусные услуги. MSSP используют операционные центры безопасности с высокой доступностью (либо на своих собственных объектах, либо у других поставщиков центров обработки данных) для предоставления услуг в круглосуточном режиме, что позволяет компании-заказчику сократить количество сотрудников оперативной безопасности, в то же время дает возможность иметь доступ к высококвалифицированным экспертам в области информационной безопасности, которых компании-заказчику не нужно нанимать и обучать для поддержания приемлемого уровня безопасности и эффективной защиты своих информационных систем и инфраструктуры [11].

2. Центр мониторинга информационной безопасности (SOC) — «структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации, и при обнаружении подозрительной активности принимают меры для предотвращения атаки» [12]. Специалисты SOC выполняют непрерывный мониторинг сети организации и проводят расследование любых потенциальных инцидентов безопасности. В случае обнаружения кибератаки они несут ответственность за принятие всех необходимых мер по ее ликвидации. Для эффективного выполнения этих мер требуются специальные технологии, которые облегчают работу аналитиков SOC.

Технологии SOC можно условно разделить на несколько уровней:

1) Сбор и анализ данных (Log Management, Big Data, Asset Management):

– Log Management – система, которая организует процесс сбора, обработки, хранения событий ИБ со всех элементов информационной инфраструктуры, а также предоставляет возможность извлечения и анализа собранной информации [13].

– Big Data в сфере информационной безопасности представляет собой подход, основанный на сборе, анализе и использовании обширных объемов разнообразных данных, полученных из различных источников, включая информационные системы, бизнес-системы, системы управления и связи, а также устройства и датчики. Эти данные характеризуются высоким объемом и быстротой обновления [13].

– Asset Management представляет собой технологию управления активами компании, включая информационные и физические ресурсы. Чем более полную информацию компания может предоставить о своих активах, тем более эффективным становится её уровень безопасности. Регулярное и актуальное ведение «инвентаризации в режиме реального времени позволяет более эффективно и оперативно устранять уязвимости, и реагировать на угрозы информационной безопасности» [11].

2) Мониторинг и анализ данных (SIEM, UEBA, TI, Machine Learning):

– «Технология SIEM решает проблему централизации мониторинга ИБ. SIEM (Security information and event management) – система для управления событиями и информацией о безопасности. Эта система объединяет в себе возможности сбора, анализа и управления информационной безопасностью в реальном времени» [13]. С использованием технологий SIEM возможно обнаружение угроз безопасности, выявление аномального поведения пользователей и систем, а также оперативная реакция на инциденты безопасности. Эта система применяет методы анализа больших данных, включая машинное обучение и искусственный интеллект, для выявления угроз и предотвращения атак на информационные системы компании. SIEM является ключевым инструментом для службы безопасности информации (SOC).

– «User and Entity Behavior Analytics (UEBA, «поведенческий анализ пользователей и сущностей») — технология выявления киберугроз, основанная на анализе поведения пользователей, а также устройств, приложений и иных объектов в информационной системе» [11]. «Основная задача UEBA — своевременно обнаруживать целевые атаки и инсайдерские угрозы. Решения

UEBA обрабатывают большой объем данных из различных источников, определяют нормальные модели поведения для каждого пользователя и объекта и уведомляют ИБ-специалистов, если замечают отклонения от этих моделей» [12].

- «Threat intelligence (данные о киберугрозах) — это информация об актуальных угрозах и группировках киберпреступников, которая позволяет организациям изучить цели, тактику и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак. Компании могут сами собирать данные о киберугрозах или заказывать информацию у сторонних поставщиков» [12].

– «Machine Learning (машинное обучение) — это подход в информационной безопасности, который позволяет создавать алгоритмы, способные обучаться на основе опыта и улучшать свою эффективность с течением времени. В информационной безопасности машинное обучение может использоваться для создания систем обнаружения и предотвращения кибератак, анализа потенциальных угроз и управления рисками» [10].

3) Автоматизация и реагирование (IRP, SOAR):

– «IRP (Incident Response Platforms) – платформа, предназначенная для автоматизации процессов мониторинга, учета и реагирования на инциденты ИБ» [14]. IRP обеспечивает автоматизацию управления инцидентами, что позволяет службам информационной безопасности и SOC ускорить процессы решения инцидентов. Это в свою очередь может заметно уменьшить время реакции на инциденты и сократить возможный ущерб для организации.

– «SOAR (Security Orchestration, Automation and Response) — класс программных продуктов, предназначенных для оркестровки систем безопасности, то есть их координации и управления ими. В частности, решения класса SOAR позволяют собирать данные о событиях информационной безопасности из различных источников, обрабатывать их и автоматизировать типовые сценарии реагирования на них». (Журнал «Информационная безопасность» [12]. Платформы SOAR позволяют объединить в единую систему множество инструментов и технологий безопасности, включая SIEM-системы, системы управления уязвимостями, средства обнаружения вторжений, решения по контролю доступа и другие. Они также обеспечивают возможность интеграции с другими бизнес-системами, что позволяет анализировать данные не только в области ИБ, но и в других сферах деятельности организации.

MSSP и SOC – это два разных подхода к обеспечению безопасности информации, которые могут быть использованы организациями, где выбор зависит от конкретных потребностей, бюджета и стратегии безопасности организации (табл. 1).

Таблица 1

Сравнение комплексных решений по организации ИБ в компании

MSSP	SOC
Сторонний поставщик услуг безопасности	Внутренний отдел или внешний провайдер услуг
Предлагает управляемые услуги по ИБ	Занимается мониторингом и обнаружением угроз ИБ
Полная зависимость от аутсорсера	Использует собственные инструменты и технологии
Предоставление широкого спектра услуг безопасности	Узкая направленность, связанная с мониторингом и обнаружением угроз
Направлен на соблюдение базовой гигиены в ИБ и требований регуляторов	Выявляет профессиональные кибератаки, заостряет внимание на стратегии и подходе злоумышленников

Источник: составлено автором на основании [11], [12].

Таким образом, MSSP направлен преимущественно на соблюдение базовой гигиены в ИБ и выполнение требований регуляторов. В основе этого решения лежит обнаружение и обработка инцидентов, что позволяет отслеживать исполнение политик ИБ и выявлять атаки различной сложности, координируя информацию с данными из ФинЦЕРТ и ГосСОПКА. В свою очередь SOC-центр выявляет профессиональные кибератаки, а также анализирует стратегии и подходы злоумышленников.

3. Экосистема информационной безопасности представляет собой комплекс взаимосвязанных и взаимодействующих элементов, процессов и технологий, направленных на обеспечение безопасности информации в организации или в целом в информационном пространстве. Эта концепция включает в себя различные компоненты, которые взаимодействуют для создания надежной и защищенной среды для

обработки, передачи и хранения информации [15, 16].

Данный подход к выстраиванию комплексной системы ИБ совмещает в себе два направления MSSP и SOC, только в случае экосистемы провайдером услуг ИБ зачастую выступает сам вендор с портфелем собственных продуктов, имеющих глубокую интеграцию между ними и позволяющим закрыть все потребности заказчика, но не исключая при этом интеграцию с продуктами по ИБ от других вендоров. Этот подход дает возможность решать дополнительные задачи, связанные с обеспечением ИБ в процессе наращивания информационной инфраструктуры компании (дополнение продуктовой линейки, улучшение функционала), что позволяет заказчику экономию бюджета на организацию ИБ.

Таким образом, проведя сравнительный анализ трех возможных подходов к организации информационной безопасности компании, можно сделать вывод о том, что экосистемный подход – это более гибкая система с пулом продуктов, интегрированных между собой, позволяющая покрывать актуальные потребности заказчика в полном объёме.

Список литературы

1. Ионина М.В. Вопросы обеспечения кибербезопасности информационной инфраструктуры таможенных органов // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. – 2023. – № 2(86). – С. 32-35. – EDN RDIEKY.
2. Интернет-портал аналитического агентства «TADVAISER» [Электронный ресурс] // URL: www.tadviser.ru/index.php/ /Статья:Информационная_безопасность_в_компании (дата обращения: 25.01.2024).
3. Афонин П.Н., Афонин Д.Н., Краснова А.И. Экономика информационной безопасности: Учебное пособие. - Российская таможенная академия; РИО Санкт-Петербургского имени В.Б. Бобкова филиала. – Санкт-Петербург: Российская таможенная академия, 2018. – 130 с. – ISBN 978-5-9590-1034-8. – EDN YRHJCA.
4. Официальный сайт компании «Ростелеком Решения» [Электронный ресурс] // URL: https://rt-solar.ru/analytics/reports/ (дата обращения: 23.11.2023).
5. Официальный сайт компании «Инфосистемы Джет» Электронный ресурс] // URL: jet.su/about/ (дата обращения: 20.11.2023).
6. Официальный сайт Государственной Думы Федерального Собрания Российской Федерации [Электронный ресурс] // URL: duma.gov.ru/news/58677/ (дата обращения: 24.01.2024).
7. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) [Электронный ресурс] // СПС «Консультант Плюс». URL: www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 28.10.2023).
8. Интернет-портал по информационной безопасности в сети [Электронный ресурс] // URL: safe-surf.ru/specialists/article/5309/687698/ (дата обращения: 17.10. 2023).
9. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс] // URL: digital.gov.ru/ru/documents/7342 (дата обращения: 15.01.2024).
10. Официальный сайт Центра компетенций по импортозамещению в сфере ИКТ [Электронный ресурс] // URL: ru-ikt.ru (дата обращения: 15.01.2024).
11. Официальный сайт исследовательской, консалтинговой компании «Gartner» [Электронный ресурс] // URL: www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider (дата обращения: 25.12.2023).
12. Официальный сайт компании «Лаборатория Касперского» [Электронный ресурс] // URL: encyclopedia.kaspersky.ru/glossary/siem/ (дата обращения: 01.11.2023).
13. Официальный сайт Ассоциации разработчиков программных продуктов «Отечественный софт» [Электронный ресурс] // URL: arppsoft.ru/members/8377/ (дата обращения: 10.11.2023).
14. Официальный сайт информационно-аналитического центра «Anti-Malware.ru» [Электронный ресурс] // URL: www.anti-malware.ru/security/irp (дата обращения: 25.11.2023).
15. Афонин Д.Н. Виртуализация, классификация и области применения в ФТС России. Возможности виртуализации. Системы и среды виртуализации: Учебное пособие. – Москва: Общество с ограниченной ответственностью "Издательство "КноРус", 2020. – 104 с. – ISBN 978-5-4365-5385-6. – EDN MMJJRO.
16. Афонин Д.Н. Возможности, перспективы и проблемы виртуализации в Федеральной таможенной службе России // Бюллетень инновационных технологий. – 2020. – Т. 4, № 2(14). – С. 52-55. – EDN HMKSVT.

Поступила в редакцию 20.01.2024

Сведения об авторе:

Ионина Марина Владимировна – старший научный сотрудник научно-исследовательского отдела Санкт-Петербургского филиала Российской таможенной академии, e-mail: ioninaspb@mail.ru.

Электронный научно-практический журнал "**Бюллетень инновационных технологий**"
(**ISSN 2520–2839**) является сетевым средством массовой информации
регистрационный номер **Эл № ФС77-73203**
по вопросам публикации в Журнале обращайтесь по адресу bitjournal@yandex.ru

рецензент

Тукеев Д.Л.

Tukeev D.L.

dimleo@inbox.ru

Михайловская военная артиллерийская академия

Mikhailovskaya Military Artillery Academy

Афонин Д.Н.

Афонин П.Н.

Afonin D.N.

Afonin P.N.

dnafonin@gmail.com

pnafonin@yandex.ru

Краснова А.И.

Krasnova A.I.

aikrasnova@mail.ru

Касторский Г.Л.

Kastorsky G.L.

mihail.kastorskii@mail.ru

Санкт-Петербургский имени В.Б. Бобкова филиал Российской таможенной академии

St. Petersburg named after V. B. Bobkov branch of the Russian Customs Academy

Начкин А.И.

Nachkin A.I.

tvakky@mail.ru

Университет при Межпарламентской Ассамблее ЕврАзЭС

University at the EurAsEC Interparliamentary Assembly

Пенина Г.О.

Penina G.O.

penkina.ru@rambler.ru

Федеральный научно-образовательный центр медико-социальной экспертизы и реабилитации им. Г.А. Альбрехта Министерства труда и социальной защиты Российской Федерации

Federal Scientific and Educational Center of Medical and Social Expertise and Rehabilitation named after G.A. Albrecht» of the Ministry of Labour and Social protection of the Russian Federation

Ягофарова И.Д.

Yagofarova I.D.

vaina3@yandex.ru

Уральский государственный экономический университет

Ural State University of Economics