УДК 004.056.5

Ю.С. Корякина, jk169@list.ru
Институт машиноведения автоматики и геомеханики НАН КР
А. А. Каныбекова, kanybekovaa21@gmail.com
Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР МЕТОДОВ ДЛЯ РЕАЛИЗАЦИИ ПОДСИСТЕМ АНТИВИРУСНОЙ ЗАЩИТЫ В СИСТЕМАХ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данная работа посвящена разработке подсистем антивирусной защиты в составе Центра мониторинга информационной безопасности (SOC). Основное внимание уделено теоретическим основам антивирусных технологий, а также детальному анализу современных инструментов для защиты от вредоносного программного обеспечения (ПО). В статье проведен обзор функциональных возможностей различных антивирусных решений, их принципов работы и эффективности в условиях современных угроз информационной безопасности (ИБ).

Ключевые слова: SOC; антивирусная защита; информационная безопасность; вредоносное ПО; обнаружение угроз; мониторинг; корпоративная сеть; защита данных; управление инцидентами; интеграция систем; производительность; ложные срабатывания; обновление баз данных; реагирование на угрозы; киберугрозы.

Введение

В современном мире киберугрозы становятся все более изощренными, что требует от Центров мониторинга безопасности (Security Operations Centers, SOC) внедрения эффективных подсистем антивирусной защиты. Актуальность разработки и совершенствования таких подсистем подтверждается рядом реальных инцидентов, продемонстрировавших уязвимость критически важных инфраструктур к вредоносным программам.

Одним из наиболее показательных примеров является атака червя Stuxnet в 2010 году. Этот вредоносный код был специально разработан для саботажа иранской ядерной программы, поражая промышленные системы управления (SCADA) и выводя из строя центрифуги для обогащения урана. Stuxnet использовал несколько уязвимостей нулевого дня и действительные цифровые подписи, что позволяло ему обходить традиционные антивирусные средства и оставаться незамеченным длительное время. Этот инцидент продемонстрировал необходимость разработки специализированных антивирусных решений, способных защищать не только офисные системы, но и промышленные объекты. С тех пор количество обнаруженных уязвимостей нулевого дня продолжает расти. В первой половине 2024 года было выявлено более 1,2 тысячи таких уязвимостей, что на 25% больше по сравнению с аналогичным периодом предыдущего года. Это свидетельствует о сохраняющейся угрозе для промышленных объектов и необходимости постоянного совершенствования мер безопасности.[9]

Еще один значимый случай — распространение программы-вымогателя WannaCry в мае 2017 года. Вирус поразил более 200 000 компьютеров в 150 странах, шифруя данные пользователей и требуя выкуп за их восстановление. Многие организации, включая медицинские учреждения и крупные корпорации, столкнулись с серьезными перебоями в работе из-за недостаточной защиты своих систем. Этот инцидент подчеркнул важность своевременного обновления антивирусных баз и операционных систем, а также необходимости интеграции антивирусных подсистем в общую стратегию кибербезопасности SOC. Несмотря на повышение осведомленности и улучшение мер защиты, программы-вымогатели продолжают представлять серьезную угрозу. Организации по-прежнему сталкиваются с атаками, приводящими к утечкам данных и финансовым потерям.

Эти примеры демонстрируют, что современные кибератаки могут иметь разрушительные последствия для различных сфер деятельности. Поэтому разработка и внедрение эффективных методов реализации подсистем антивирусной защиты в SOC является критически важной задачей для обеспечения информационной безопасности. [1]

В отчете State of Threat Hunting от компании Intrusion определили 5 основных проблем, с которыми сталкиваются центры управления безопасностью (Security Operations Centers, SOC). По мнению участников опроса, самыми серьезными проблемами являются следующие:

- Обнаружение современных угроз
- Нехватка специалистов по безопасности для устранения угроз
- Слишком много времени тратится на ложные срабатывания
- Недостаточная уверенность в том, что средства автоматизации способны выявить все угрозы
- Медленное время реагирования на современные угрозы.

Рисунок 1 — Основные проблемы SOC

1. Недостаточная способность обнаруживать современные угрозы.

Продвинутые угрозы, использующие методы уклонения, способны поразить многие средства обнаружения угроз, имеющиеся в арсенале SOC. В прошлом высокотехнологичные кибератаки были делом рук исключительно организованных киберпреступных групп. Однако сегодня современные кибератаки могут исходить и от более зловещих противников. Появление угроз со стороны иностранных государств радикально изменило ландшафт киберугроз в худшую сторону.

Обладая огромным человеческим, технологическим и финансовым капиталом, эти субъекты способны развертывать современные постоянные угрозы (APT), в основном для шпионажа и диверсионных кампаний. APT — это глубоко законспирированные группы угроз, которые могут проникать в хорошо защищенные инфраструктуры и сохраняться в них столько, сколько им нужно. Поскольку в отчете Microsoft Digital Defense Report за 2022 год говорится о том, что кибератаки со стороны угрожающих групп иностранных государств стали более изощренными, необходимость обнаружения современных угроз стала еще более важной.

Для того чтобы SOC мог обнаруживать эти высокотехнологичные угрозы, необходимы мощные, но обычно дорогостоящие инструменты обнаружения угроз. Для их использования

также необходим опыт. Без необходимых знаний и опыта ваши средства безопасности не смогут быть оптимизированы для обнаружения APT и других современных угроз.

2. Нехватка специалистов по безопасности для устранения угроз.

В настоящее время организации сталкиваются с проблемой нехватки специалистов по кибербезопасности, из-за которой в прошлом году не было заполнено 3,5 миллиона вакансий в сфере кибербезопасности. Даже если бы вы хотели нанять сотрудников по кибербезопасности для своего SOC и могли бы себе это позволить, то все равно никого бы не нашлось.

Этот недостаток усугубляется все более широким внедрением таких методов работы, как удаленная работа и использование собственных устройств (BYOD), а также таких технологий, как облачные вычисления, которые не только расширяют поверхность атаки, но и повышают сложность всей ИТ-среды.

Нехватку специалистов по кибербезопасности можно компенсировать автоматизацией. А именно средствами или продуктами безопасности, способными функционировать без постоянного наблюдения сотрудников.

3. Слишком много времени тратится на предупреждения о ложных срабатываниях.

Растущая сложность и разнообразие угроз в сочетании с постоянным шквалом маркетинговых кампаний от поставщиков средств защиты подтолкнули организации к накоплению арсенала инструментов безопасности. Сейчас у организаций в среднем 76 инструментов, многие из которых генерируют массу предупреждений, и значительная часть из них является ложными срабатываниями.

Одна только сортировка, обогащение, обработка и анализ легитимных оповещений уже может оказаться непосильной задачей. Куда больше, если вам приходится иметь дело еще и с ложными срабатываниями? Ложноположительные оповещения могут помешать вам проанализировать и выявить текущую кибератаку. Они могут ввести аналитиков в заблуждение, заставив их пуститься в бесполезную, отнимающую много ресурсов погоню.

Кроме того, слишком большое количество ложных срабатываний может сделать аналитиков SOC более восприимчивыми к усталости от оповещений. Когда наступает усталость от оповещений, сотрудники службы безопасности начинают испытывать разочарование, стресс и склонность к выгоранию. Это, в свою очередь, может заставить сотрудников отключить оповещения (что позволит большему количеству угроз избежать обнаружения) или, что еще хуже, покинуть вашу организацию в поисках более благоприятных условий работы.

4. Отсутствие уверенности в том, что средства автоматизации способны отразить все угрозы.

Автоматизация имеет решающее значение для операций безопасности. Автоматизируя рабочие процессы, аналитики SOC могут сократить время, затрачиваемое на выполнение определенных функций, таких как анализ угроз, мониторинг угроз, обнаружение угроз, анализ угроз, реагирование на инциденты и так далее. Это помогает повысить скорость и эффективность выполнения задач. Таким образом, автоматизация в какой-то мере помогает решить проблему нехватки кадров в сфере кибербезопасности.

Но есть одна загвоздка. Автоматизация сильно зависит от надежности отдельных компонентов. Например, если данные, используемые для обнаружения угроз, состоят в основном из ложных срабатываний, это только введет в заблуждение и запутает аналитиков угроз. Аналогичным образом, если вы слишком полагаетесь на автоматизированный процесс, а он генерирует множество ложноотрицательных результатов, вы просто приобретете ложное чувство безопасности.

5. Медленное время реагирования на современные угрозы.

Ложные срабатывания и отсутствие надежных автоматизированных средств обнаружения угроз не позволяют сотрудникам службы безопасности оперативно реагировать на современные угрозы. Но чем дольше киберугроза остается незамеченной, тем больше у нее возможностей нанести значительный ущерб вашей организации.

К сожалению, в прошлогоднем отчете Cost of a Data Breach среднее время обнаружения и локализации утечки данных составило 277 дней. Это слишком долго. В том же отчете говорится, что средняя экономия, которую вы получаете при локализации утечки за 200 дней или менее, составляет 1,12 млн долларов. Очевидно, что если вы сможете сократить время на обнаружение угрозы и реагирование на нее, то получите значительную экономию средств. И наоборот, более длительное время обнаружения и реагирования приводит к увеличению затрат.

В рамках проекта «Разработки подсистемы антивирусной защиты SOC» можно выделить следующие возможные решения проблем, упомянутые выше.[2]

1) Обнаружение современных угроз.
   - Внедрение поведенческого анализа (Behavior-Based Detection) для выявления аномальной активности.
   - Интеграция с Threat Intelligence платформами для получения актуальных индикаторов компрометации (IoC).
2) Нехватка специалистов по безопасности для устранения угроз.
   - Интеграция антивирусной системы с SOC SIEM для централизованного анализа событий.
   - Использование автоматических патчей и обновлений антивирусных баз данных без участия специалистов.
3) Слишком много времени тратится на ложные срабатывания.
   - Использование интеллектуальных фильтров для уменьшения false positives.
   - Настройка поведенческого анализа с учетом специфики организации, чтобы сократить количество ложных тревог.
4) Недостаточная уверенность в автоматизированных средствах обнаружения.
   - Разработка гибридной модели обнаружения, объединяющей сигнатурный, эвристический и поведенческий анализ.
   - Интеграция с Threat Intelligence для обогащения данных о новых атаках.
5) Медленное время реагирования на современные угрозы.
   - Автоматическая изоляция зараженных узлов и устранение вредоносного ПО без вмешательства оператора.
   - Настройка реактивных политик для автоматической блокировки вредоносных процессов и подключения зараженных систем к карантинной сети.

Для поэтапного решения вышеперечисленных проблематик необходимо ознакомиться с методами антивирусной защиты SOC. Методы делятся на несколько этапов:

Классические сигнатурные методы

Обнаружение на основе сигнатур остается основополагающим подходом к антивирусной защите в Центрах управления безопасностью (SOC). Этот метод основан на сравнении файлов, кода и процессов с заранее определенной базой данных известных сигнатур вредоносного ПО, что обеспечивает быстрое выявление и устранение ранее распознанных угроз. Благодаря своей эффективности и низким вычислительным затратам сигнатурное обнаружение остается важным компонентом современных стратегий кибербезопасности.

Однако его основное ограничение заключается в неспособности обнаружить угрозы «нулевого дня» и полиморфные вредоносные программы, которые часто изменяют свой код, чтобы обойти распознавание по сигнатурам. Для решения этих проблем современные SOC используют эвристический анализ, поведенческий мониторинг и модели машинного

обучения в дополнение к традиционным методам, основанным на сигнатурах. Кроме того, платформы Threat Intelligence позволяют в режиме реального времени обновлять и коррелировать возникающие индикаторы угроз, повышая точность и адаптивность механизмов обнаружения.

На рисунке 2 поэтапно описан традиционный антивирусный процесс, основанный на сигнатурном методе:

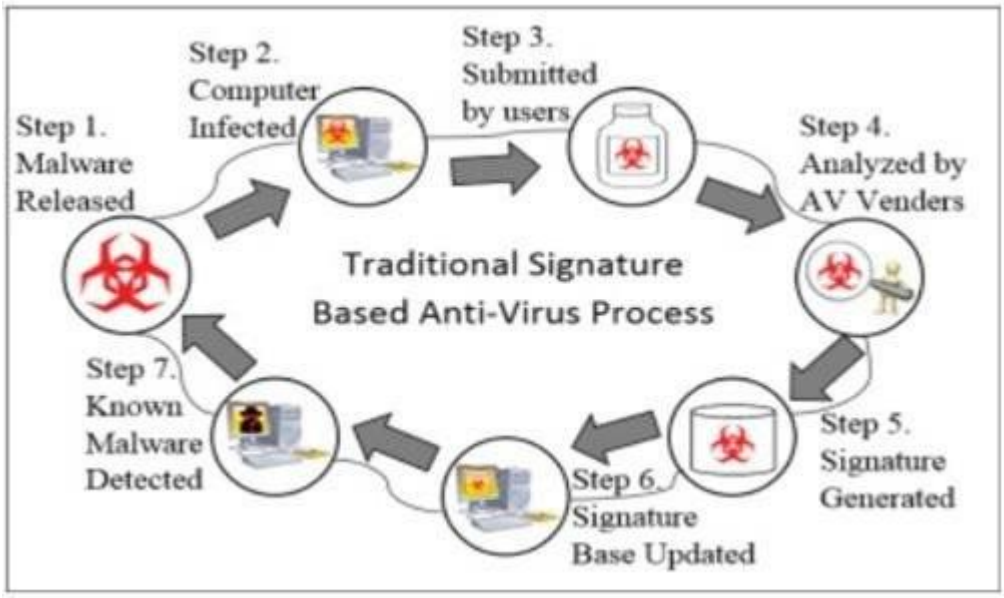

Рисунок 2 — Традиционный антивирусный процесс, основанный на сигнатурах

1. Выпуск вредоносного ПО.
2. Заражение компьютера.
3. Отправка пользователями.
4. Анализ антивирусными вендорами.
5. Генерация сигнатуры.
6. Обновление базы сигнатур.
7. Обнаружение известного вредоносного ПО.

Эвристические методы

Эвристические методы антивирусной защиты представляют собой проактивный подход к выявлению потенциальных угроз путем анализа поведения, структуры и атрибутов файлов, а не только на основе известных сигнатур. В Центрах управления безопасностью (SOC) эти методы необходимы для обнаружения новых, неизвестных или модифицированных вредоносных программ, которые системы на основе сигнатур могут пропустить. Эвристика предполагает оценку файлов на наличие подозрительных шаблонов, таких как необычное выполнение кода или аномальное поведение системы, что может указывать на наличие вредоносной активности.

В отличие от традиционного обнаружения на основе сигнатур, которое требует предварительного знания об угрозе, эвристические методы позволяют выявлять атаки «нулевого дня» и полиморфные вредоносные программы, которые эволюционируют, чтобы обойти статические средства защиты. Эвристика поведения расширяет эти возможности, динамически анализируя действия программ в режиме реального времени, что позволяет выявлять подозрительное поведение, например попытки несанкционированного доступа или изменения файловой системы до того, как будет нанесен значительный ущерб.

Хотя эвристические методы позволяют повысить эффективность обнаружения, они могут генерировать ложные срабатывания, поскольку основаны на распознавании образов, что может привести к тому, что вполне безопасное ПО будет считаться вредоносным. Чтобы смягчить эту проблему, SOC объединяют эвристический анализ с машинным обучением, анализом угроз и контекстным анализом, повышая точность и снижая нагрузку на аналитиков безопасности. Такой многоуровневый подход позволяет SOC оперативно реагировать на возникающие угрозы, повышая общий уровень защиты от сложных кибератак.

Далее представлена схема на рисунке 3 – поэтапный принцип работы эвристического метода антивирусной защиты:

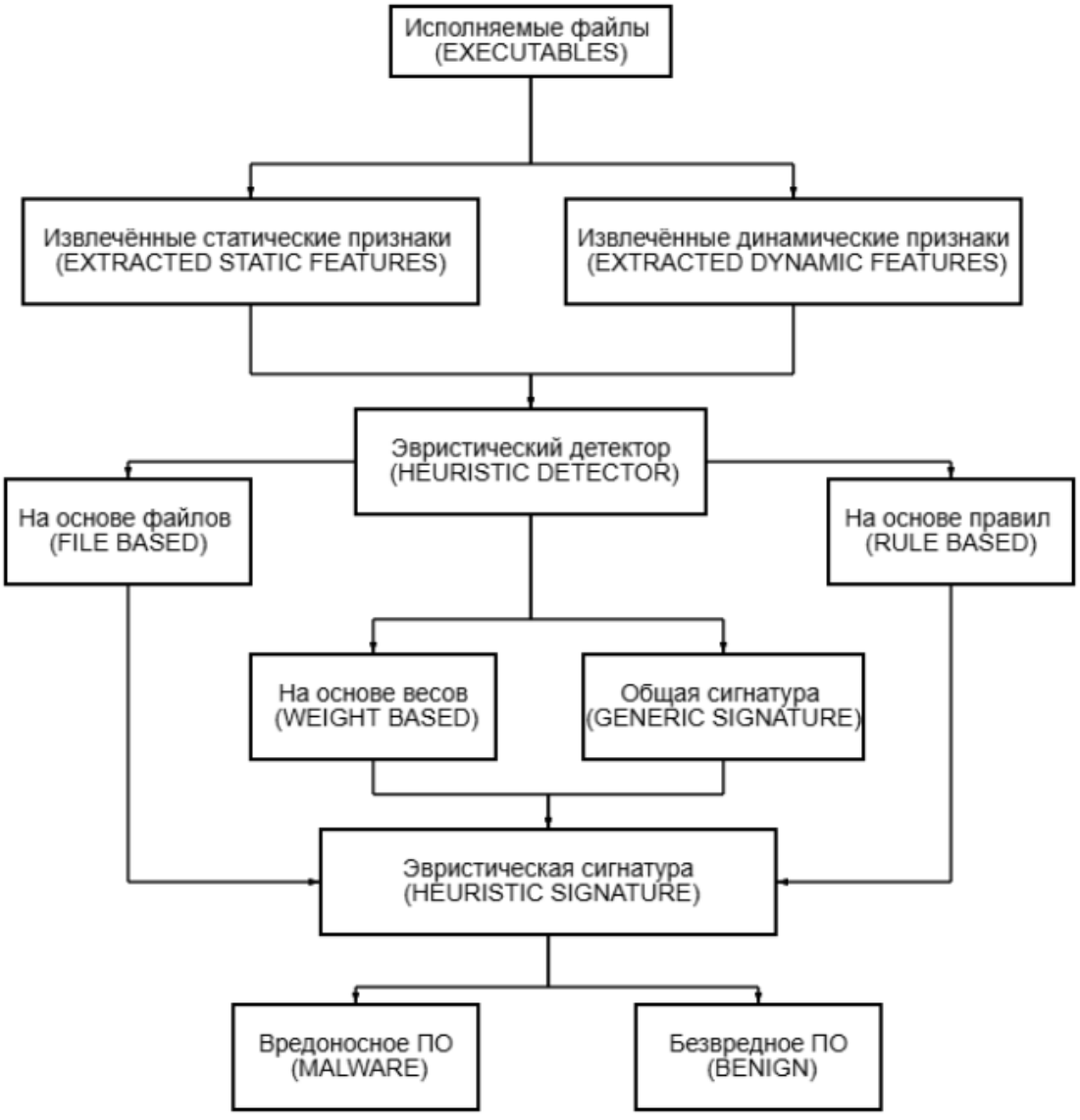

Рисунок 3 — Принцип работы эвристического метода

Поведенческий анализ и мониторинг активности

Поведенческий анализ и мониторинг играют важную роль в антивирусной защите в Центрах управления безопасностью (SOC), позволяя обнаруживать угрозы, которые традиционные методы, основанные на сигнатурах, могут пропустить. В отличие от статических методов обнаружения поведенческий анализ фокусируется на действиях и шаблонах, демонстрируемых программами во время выполнения. Этот метод позволяет антивирусным системам в режиме реального времени выявлять «вредоносное поведение», например, несанкционированные модификации файлов, сетевую активность или попытки

использования уязвимостей системы, даже в ранее неизвестных вариантах вредоносного ПО.

Наблюдая и анализируя такое поведение, SOC могут обнаруживать «атаки нулевого дня», полиморфные вредоносные программы и передовые постоянные угрозы (APT), которые постоянно совершенствуются, чтобы обойти обычные средства защиты. Поведенческий мониторинг обычно осуществляется с помощью инструментов Endpoint Detection and Response (EDR), которые непрерывно отслеживают конечные точки и выдают предупреждения о подозрительных действиях, способствуя тем самым быстрому обнаружению угроз и реагированию на них.

Несмотря на высокую эффективность, поведенческий анализ может давать ложные срабатывания из-за сложности различения легитимных и вредоносных действий. Чтобы смягчить эту проблему, SOC часто объединяют поведенческий мониторинг с контекстным анализом, машинным обучением и анализом угроз для повышения точности обнаружения. Такой подход повышает способность SOC реагировать на сложные кибератаки, обеспечивая критически важный уровень защиты от возникающих и развивающихся угроз.

Далее на рисунке 4 представлен поэтапный принцип работы поведенческого анализа и мониторинга активности:

Рисунок 4 — Принцип работы метода

Комплексный подход: сочетание различных методов

Комплексный подход к антивирусной защите в Центрах управления безопасностью (SOC) предполагает интеграцию нескольких механизмов обнаружения и защиты для обеспечения многоуровневой защиты от широкого спектра киберугроз. Эта стратегия сочетает традиционное обнаружение на основе сигнатур, эвристический анализ, поведенческий мониторинг и анализ сетевого трафика, создавая многогранную систему защиты, которая повышает способность выявлять и устранять как известные, так и неизвестные угрозы.

Обнаружение на основе сигнатур обеспечивает высокую точность обнаружения ранее идентифицированных вредоносных программ, в то время как эвристические методы позволяют выявлять новые или модифицированные угрозы на основе подозрительных шаблонов кода. Поведенческий анализ, в свою очередь, отслеживает активность в реальном времени, чтобы обнаружить аномальные действия, указывающие на потенциальную угрозу, например несанкционированный доступ или манипуляции с системой. Анализ сетевого трафика направлен на выявление аномальных схем обмена данными, которые могут свидетельствовать об утечке данных, деятельности ботнетов или боковом перемещении злоумышленников.

Комбинируя эти методы, SOC могут эффективно устранить недостатки каждого из них в отдельности. Системы, основанные на сигнатурах, усиливаются эвристикой и поведенческим анализом, которые позволяют обнаружить ранее неизвестные или полиморфные вредоносные программы. Аналогичным образом анализ сетевого трафика обеспечивает дополнительный уровень видимости для обнаружения угроз, пытающихся обойти защиту конечных точек.

Далее представлена таблица 1 – роли и взаимодействия различных методов в комплексном подходе.

Таблица 1 – Комплексный подход

Комплексный метод				
Сигнатурный метод	**Эвристический метод**	**Поведенческий анализ**	**Мониторинг и анализ логов**	**Взаимодействие всех методов**
Проверка файлов по базе известных вирусов	Анализирует структуру и код файлов	Мониторинг активности программ и процессов	Собирает события с разных систем (EDR, Firewall, IDS)	Сигнатуры → быстрый отклик на известные угрозы
Быстрое обнаружение известных угроз	Определяет подозрительные команды и поведение	Выявляет аномалии (подозрительные изменения в ОС, сети, файлах)	Коррелирует данные и выявляет комплексные атаки	Эвристика → находит скрытые угрозы
Не выявляет новые и мутирующие угрозы	Возможны ложные срабатывания	Требует мощных ресурсов и глубокой аналитики	сложность настройки и требует SOC-аналитиков	Поведение → выявляет атаки нулевого дня

Технологии и инструменты для реализации подсистемы антивирусной защиты

Инструменты для данной цели рассматриваются open-source и коммерческие решения. Необходимо проанализировать эти категории и выявить наиболее подходящий.

Open-source решения или решения с открытым исходным кодом. В качестве рассматриваемого примера берутся такие инструменты, как ClamAV и Zeek. Эти решения широко применяются в условиях, когда первоочередное внимание уделяется экономической эффективности, гибкости и общинному развитию.

Основное преимущество открытых решений — их бесплатная доступность, устранение лицензионных сборов для частных лиц или организаций с ограниченным бюджетом. Этот аспект экономии средств особенно привлекателен для небольших предприятий или научно-исследовательских учреждений.

Открытые решения, такие как ClamAV и Zeek, предоставляют обширные возможности для настройки, позволяя пользователям изменять программное обеспечение в соответствии с конкретными потребностями безопасности. Организации могут изменять конфигурации, интегрировать с другими инструментами и даже разрабатывать пользовательские сценарии обнаружения, предлагая уровень гибкости, не всегда доступный при коммерческих решениях. [4]

Далее в виде таблицы представлены основные преимущества и недостатки обоих решений. [5]

Таблица 2 — Преимущества и недостатки ClamAV

Преимущества	**Недостатки**
Кросс-платформенность: Поддерживает различные операционные системы, включая Unix-подобные системы, OpenVMS, Microsoft Windows и macOS	Ограниченная эффективность обнаружения: в тестах 2008 года ClamAV показал низкие результаты в обнаружении вредоносных программ и rootkit-ов. В исследовании 2022 года его эффективность составила 59,94% при обнаружении распространенных типов вредоносного ПО
Открытый исходный код: распространяется под лицензией GNU General Public License, что позволяет пользователям и разработчикам вносить изменения и улучшения	Отсутствие официального графического интерфейса: ClamAV не предоставляет собственного графического интерфейса, что может затруднить использование для некоторых пользователей. Однако существуют сторонние GUI, такие как KlamAv для KDE и ClamTk для GNOME
Интеграция с почтовыми серверами: предоставляет интерфейс Milter для Sendmail и поддерживает большинство форматов почтовых файлов, что делает его полезным для сканирования электронной почты на наличие вирусов	Ограниченная защита в реальном времени: хотя ClamAV предоставляет возможности сканирования "на лету", его защита в реальном времени может быть не такой эффективной, как у некоторых коммерческих антивирусных решений
Поддержка различных форматов файлов: может анализировать сжатые файлы (RAR, ZIP, Gzip, Bzip2), форматы OLE2, Cabinet, CHM и другие, а также файлы форматов HTML, RTF и PDF	Зависимость от обновлений базы данных: эффективность ClamAV зависит от регулярного обновления вирусных баз данных. В некоторых регионах доступ к обновлениям может быть ограничен, что снижает эффективность защиты

Таблица 3 — Преимущества и недостатки Zeek

Преимущества	**Недостатки**
Глубокий анализ сетевого трафика: Zeek осуществляет детальный анализ различных протоколов и взаимодействий, что позволяет выявлять подозрительные или вредоносные действия в сети	Сложность настройки и использования: для эффективного использования Zeek требуются определенные знания и навыки в области сетевой безопасности и администрирования, что может быть сложным для неопытных пользователей

Гибкость и расширяемость: Zeek предоставляет возможности для написания пользовательских скриптов, что позволяет адаптировать его под конкретные нужды и сценарии использования	Ответственность за обслуживание: пользователь несет ответственность за обслуживание и обновление сервера с установленным Zeek, а также за резервное копирование данных
Интеграция с другими инструментами: Zeek может интегрироваться с различными системами управления событиями информационной безопасности (SIEM), такими как Splunk или Elastic, для дополнительного анализа данных	Потребление ресурсов: при высоких нагрузках или в больших сетях Zeek может потреблять значительные системные ресурсы, что требует соответствующей инфраструктуры для обеспечения производительности
Открытый исходный код: Zeek является бесплатным проектом с открытым исходным кодом, что позволяет сообществу вносить вклад в его развитие и адаптировать под специфические требования	Отсутствие графического интерфейса: Zeek не предоставляет собственного графического интерфейса, что может затруднить его использование для некоторых пользователей. Однако существуют сторонние решения для визуализации данных.

В целом данные инструменты не представляют собой антивирусной системы по отдельности, но при объединении и комплексном использовании получается эффективное решение [6]. Однако даже вместе они не смогут полностью закрыть основные проблемы, которые рассматриваются в данной статье. Поэтому необходимо разобрать и коммерческие решения. В качестве примера будут рассмотрены антивирусные системы ESET и Kaspersky.

ESET и Kaspersky — два известных коммерческих антивирусных решения, обеспечивающих комплексную защиту от широкого спектра киберугроз. Оба решения обладают уникальными возможностями.

И ESET, и Kaspersky используют передовые многоуровневые механизмы защиты, включая сигнатурное обнаружение, эвристику, поведенческий анализ и облачную аналитику угроз, обеспечивая надежную защиту от известных и возникающих угроз, таких как вредоносное ПО, программы-вымогатели и атаки «нулевого дня». Далее также, в виде таблицы, будут представлены их преимущества и недостатки.

Таблица 4 —Преимущества и недостатки антивирусной системы ESET

Преимущества	**Недостатки**
Минимальное влияние на системные ресурсы: ESET известен своей эффективностью и низким потреблением ресурсов, что обеспечивает быструю работу системы	Ограниченный функционал в базовой версии: базовая версия ESET NOD32 предоставляет только основные функции защиты без дополнительных возможностей
Высокая скорость сканирования: быстрое обнаружение и удаление угроз благодаря оптимизированному механизму сканирования	Отсутствие некоторых дополнительных функций: в сравнении с конкурентами ESET может не предоставлять такие функции, как VPN

	или менеджер паролей
Регулярные обновления: частые обновления вирусных баз данных обеспечивают защиту от новых угроз	Ограниченная защита от фишинга: защита от фишинговых сайтов может быть менее эффективной по сравнению с другими антивирусами
Кросс-платформенность: поддержка различных операционных систем, включая Windows, macOS и Linux	Интерфейс пользователя: интерфейс может показаться сложным для неопытных пользователей [7]

Таблица 5 —Преимущества и недостатки Kaspersky

Преимущества	**Недостатки**
Высокий уровень обнаружения угроз: Kaspersky регулярно получает высокие оценки в независимых тестах за эффективность обнаружения и блокировки вредоносных программ	Высокое потребление системных ресурсов: некоторые пользователи отмечают, что Kaspersky может замедлять работу системы из-за значительного потребления ресурсов
Широкий набор функций: кроме базовой антивирусной защиты, Kaspersky предлагает дополнительные функции, такие как родительский контроль, защита онлайн-платежей и VPN	Потенциальные конфликты с другим ПО: Kaspersky может быть несовместим с некоторыми другими антивирусными и антишпионскими программами, что может вызвать конфликты при совместном использовании
Регулярные обновления и поддержка: частые обновления вирусных баз и оперативная техническая поддержка обеспечивают актуальность защиты	Ограниченная совместимость с некоторыми системами: Kaspersky может быть несовместим с определенными операционными системами или устаревшим оборудованием, что ограничивает его использование на некоторых устройствах
Интуитивно понятный интерфейс: пользовательский интерфейс Kaspersky разработан для удобства и простоты использования, что облегчает настройку и управление защитой	Потенциальные риски безопасности: в некоторых странах возникали опасения по поводу безопасности использования продуктов Kaspersky из-за предполагаемых связей с российскими государственными структурами, что привело к ограничениям на использование их ПО в государственных учреждениях
Интеграция с другими системами безопасности: Kaspersky предоставляет возможности для интеграции с другими решениями безопасности, что позволяет создавать комплексные системы защиты	Стоимость лицензии: полная версия Kaspersky с расширенным функционалом может быть дороже по сравнению с некоторыми конкурентами, что может быть существенным фактором для домашних пользователей и небольших предприятий.[8]

Ведущие антивирусные решения, такие как ESET и Kaspersky, используют гибридные модели обнаружения, сочетающие сканирование на основе сигнатур с поведенческим анализом и облачными системами репутации. Такой многоуровневый подход обеспечивает надежную защиту как от известных, так и от развивающихся киберугроз, укрепляя позиции организаций по защите от сложных векторов атак. Но при выборе антивирусного решения для защиты **Security Operations Center (SOC)** необходимо учитывать множество факторов. Основываясь на сравнении коммерческих решений, можно составить следующую таблицу:

Таблица 6 –– Сравнение и анализ коммерческих решений

Проблема в SOC	**Решение ESET**	**Решение Kaspersky**
Обнаружение современных угроз	ESET обеспечивает обнаружение современных угроз благодаря регулярным обновлениям и проактивной защите	Kaspersky предоставляет расширенные функции для обнаружения сложных угроз, включая APT, с помощью команды GReAT.
Нехватка специалистов по безопасности для устранения угроз	ESET предлагает автоматизацию некоторых процессов, но может потребоваться дополнительная настройка и мониторинг	Kaspersky предоставляет комплексные решения с автоматизацией и аналитикой, что снижает нагрузку на специалистов SOC
Слишком много времени тратится на ложные срабатывания	ESET стремится минимизировать ложные срабатывания, но в некоторых случаях может потребоваться ручная проверка	Kaspersky известен низким уровнем ложных срабатываний благодаря точным алгоритмам обнаружения и регулярным обновлениям
Недостаточная уверенность в том, что средства автоматизации способны выявить все угрозы	ESET предоставляет базовые средства автоматизации, но для полной уверенности может потребоваться дополнительная настройка	Kaspersky предлагает расширенные средства автоматизации и аналитики, повышающие уверенность в обнаружении всех угроз
Медленное время реагирования на современные угрозы	ESET обеспечивает быстрое реагирование на известные угрозы, но сложные атаки могут требовать дополнительного вмешательства	Kaspersky предоставляет оперативное реагирование на современные угрозы благодаря постоянному мониторингу и обновлениямхъ

Вследствие всего можно отметить, что данные решения подходят для минимизации основных проблем SOC, однако все же имеют свои нюансы. Таким образом, для эффективного функционирования Центра мониторинга информационной безопасности (SOC) рекомендуется использовать комбинацию решений от ESET и Kaspersky. ESET обеспечивает минимальное влияние на системные ресурсы и высокую скорость сканирования, что полезно для поддержания производительности системы. Kaspersky, в

свою очередь, предоставляет расширенные функции обнаружения сложных угроз и автоматизации, что снижает нагрузку на специалистов по безопасности и повышает эффективность реагирования на инциденты. Совместное использование этих антивирусных систем позволит компенсировать недостатки каждой из них.

Для ясности приведена схема взаимодействия подсистемы с SOC.

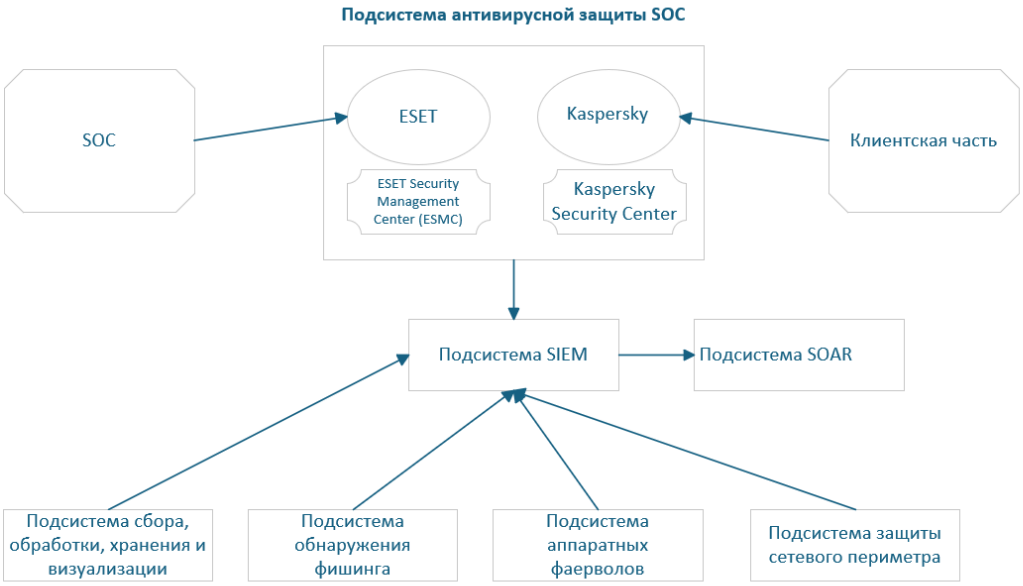

Рисунок 5—Структурная схема подсистемы антивирусной защиты

Принцип работы антивирусной защиты.

Все антивирусные решения (ESET и Kaspersky) управляются через свои серверы (ESMC и Kaspersky Security Center). Серверы управления интегрированы с SIEM для централизованного мониторинга. Антивирусные клиенты на рабочих станциях и серверах передают данные о состоянии системы и инцидентах на соответствующие серверы управления. Далее серверы управления передают сводные данные в SIEM-систему SOC. После чего все события поступают в SIEM, где выполняется корреляция и анализ, и интегрируются с SOAR для автоматического реагирования (блокировка, создание тикетов).

На следующей схеме более детально обрисован принцип защиты клиентской части и SOC (рис. 6):

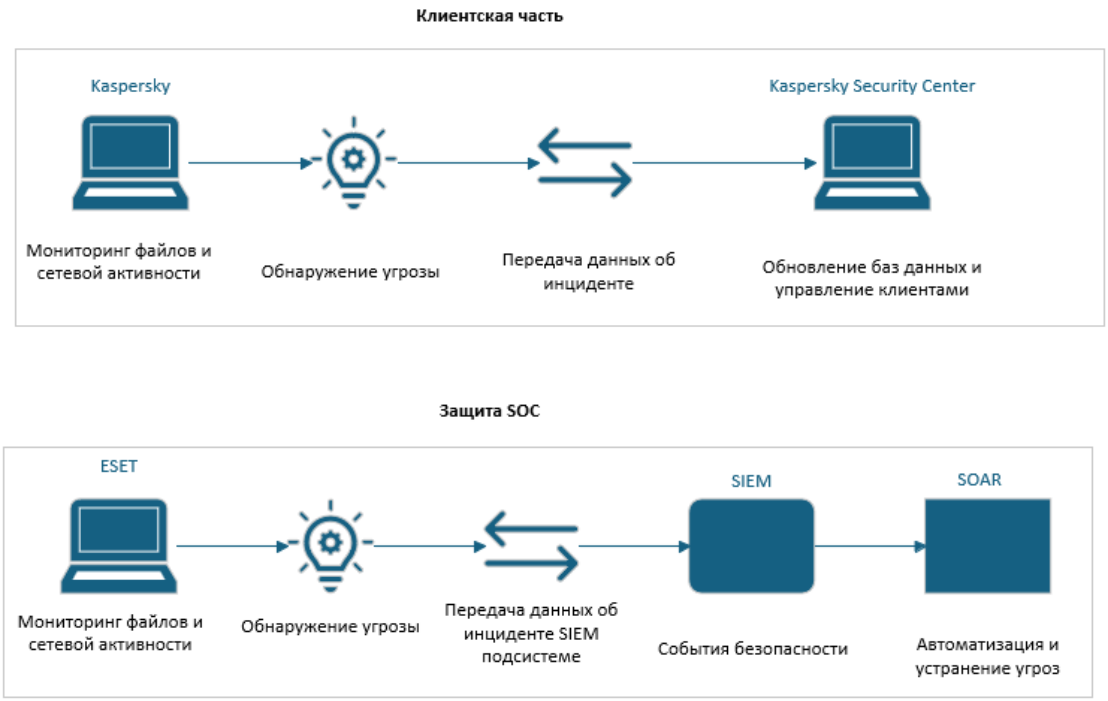

Рисунок 6—Логическая схема защиты клиентских устройств

Клиентская часть: агенты проводят мониторинг файловой системы, сетевой активности и процессов на наличие вредоносного ПО. При обнаружении угрозы агент передает данные на сервер управления (Kaspersky Security Center). После чего сервер управления обновляет базы данных угроз и отправляет данные в SIEM-систему для централизованного мониторинга.

Защита SOC: SIEM анализирует события, выполняет корреляцию с другими источниками данных и создает предупреждения о потенциальных угрозах. При подтверждении угрозы данные передаются в SOAR-систему для автоматического реагирования (например, изоляция зараженного устройства или блокировка вредоносного процесса).

Резервный вариант

В добавок ко всему прочему в разработке подсистемы антивирусной защиты учитывается фактор непредвиденных ситуаций, т.е. существует резервный вариант. Если основные инструменты (ESET, Kaspersky) перестанут функционировать, на замену им будет использоваться комплекс из решений с открытым исходным кодом (к примеру, ClamAV и Zeek) (рис. 7):

Рисунок 7— Структурная схема подсистемы антивирусной защиты с использованием резервной подсистемы

В ходе проведенного исследования были рассмотрены основные проблемы, влияющие на эффективность работы подсистем антивирусной защиты в SOC: недостаточная способность обнаружения современных угроз, нехватка специалистов по кибербезопасности, высокая частота ложных срабатываний, ограниченные возможности автоматизации и медленное время реагирования на инциденты. Для решения этих проблем были изучены различные методы антивирусной защиты, включая сигнатурные и эвристические подходы, поведенческий анализ и комплексные гибридные модели.

Проведенное сравнение бесплатных и коммерческих решений показало, что наиболее оптимальной стратегией является использование комплекса антивирусных систем на основе сочетания продуктов ESET и Kaspersky. Эти решения обеспечивают высокую точность обнаружения и автоматизацию реагирования, минимизируя ложные срабатывания и снижая нагрузку на специалистов. В качестве резервного варианта предложено использовать бесплатные решения с открытым исходным кодом, такие как ClamAV и Zeek, которые могут обеспечить базовый уровень защиты при отказе коммерческих продуктов.

Таким образом, комплексный подход к антивирусной защите SOC с использованием как коммерческих, так и бесплатных решений позволяет значительно повысить устойчивость к киберугрозам, сократить время реагирования на инциденты и обеспечить надежное функционирование инфраструктуры информационной безопасности.

Литература

1. https://itta.info/ru/10-samyx-vpechatlyayushhix-kiberatak-v-istorii/ (дата обращения 05.01.2025 г.).
2. https://www.intrusion.com/blog/the-biggest-challenges-for-socs/ (дата обращения 15.01.2025 г.).
3. https://www.anti-malware.ru/proactive_test_2010 (дата обращения 20.01.2025 г.).
4. https://www.clamav.net/ https://zeek.org/ (дата обращения 30.01.2025 г.).
5. https://en.wikipedia.org/wiki/ClamAV (дата обращения 05.02.2025 г.).
6. https://itshaman.ru/it-programmy-dlya-linux/4866/zeek-analiz-setevogo-trafika-s-otkrytym-iskhodnym-kodom-dlya-monitoringa-bezopasnosti (дата обращения 10.02.2025 г.).
7. https://www.eset.com (дата обращения 15.02.2025 г.).

8. https://www.kaspersky.com (дата обращения 20.02.2025 г.).
9.https://securitymedia.org/news/kolichestvo-uyazvimostey-nulevogo-dnya-vozroslo-na-chetvert-v-pervoy-polovine-2024 (дата обращения 05.03.2025 г.).