ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.21822/2073-6185-2025-52-4-23-38 Оригинальная статья/ Original article

Интеграция и адаптация открытых средств мониторинга для обнаружения аномальной пользовательской активности в Astra Linux Special Edition

И.И. Андреев[1], С.О. Иванов[1], Т.Н. Копышева[1], М.В. Никандров[2], Т.Н. Смирнова[1]
[1]Чувашский государственный университет имени И.Н. Ульянова,
[1]428015, г. Чебоксары, Московский пр-т, д. 15, Россия,
[2]ООО «Интеллектуальные сети»,
[2]428003, г. Чебоксары, ул. Пристанционная, д. 1, корп. 9, Россия

Резюме. Цель. Разработка и оценка метода интеграции open-source средств мониторинга для обнаружения аномальной активности в Astra Linux Special Edition с учетом встроенных механизмов защиты. М**етод.** Исследование основано на интеграции инструментов Wazuh, OSSEC, Suricata и audit.d; адаптации правил под специфику Astra Linux; тестировании на основе техник MITRE ATT&CK; анализе по стандартам ГОСТ Р 59548-2022 и NIST SP 800-92. **Результат.** Разработана методика интеграции и адаптации open-source средств мониторинга (Wazuh, Suricata, OSSEC) для обнаружения аномальной пользовательской активности в операционной системе специального назначения Astra Linux Special Edition. Осуществлена адаптация правил корреляции событий под встроенные механизмы защиты ОС (мандатный контроль, аудит Parsec) и интеграция с внешними платформами анализа угроз (VirusTotal, URLhaus). **Вывод.** Предложенная методика обеспечивает эффективное обнаружение аномальной активности в Astra Linux. Адаптация Open-Source решений позволила достичь соответствия требованиям безопасности. Система демонстрирует высокую точность при минимальном количестве ложных срабатываний. Рекомендуется для организаций, переходящих на отечественные операционные системы специального назначения.

Ключевые слова: кибератака; активность пользователя; мониторинг активности; системы мониторинга; Astra Linux Special Edition

Для цитирования: И.И. Андреев, С.О. Иванов, Т.Н. Копышева, М.В. Никандров, Т.Н. Смирнова. Интеграция и адаптация открытых средств мониторинга для обнаружения аномальной пользовательской активности в Astra Linux Special Edition. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(4):23-38. DOI:10.21822/2073-6185-2025-52-4-23-38.

Integration and Adaptation of Open-Source Monitoring Tools for Detecting Anomalous User Activity in Astra Linux Special Edition

I.I. Andreev[1], S.O. Ivanov[1], T.N. Kopysheva[1], M.V. Nikandrov[2], T.N. Smirnova[1]
[1]I.N. Ulyanov Chuvash State University,
[1]15 Moskovsky Ave, Cheboksary 428015, Russia,
[2]LLC "Intellectual networks",
[2]1 Pristantsionnaya Str., 1, bldg. Cheboksary 428003, Russia

Abstract. Objective. Development and evaluation of a method for integrating open-source monitoring tools for detecting abnormal activity in Astra Linux Special Edition, taking into account the built-in protection mechanisms. **Method.** Integration of Wazuh, OSSEC, Suricata and audit tools.d; adaptation of the rules to the specifics of Astra Linux; testing based on MITRE ATT&CK techniques; analysis according to GOST R 59548-2022 and NIST SP 800-92 standards. **Result.** A methodology for integrating and adapting open-source monitoring tools (Wazuh, Suricata, OSSEC) to detect abnormal user activity in the special-purpose operating system Astra Linux Special Edition. Adaptation of event correlation rules to the built-in OS protection mechanisms

(mandatory control, Parsec audit) and integration with external threat analysis platforms (VirusTotal, URLhaus). **Conclusion.** This methodology ensures effective detection of abnormal activity in Astra Linux. Adaptation of open-source software enabled compliance with security requirements. The system demonstrates high accuracy with minimal false positives. It is recommended for organizations migrating to domestic special-purpose operating systems.

Keywords: cyberattack; user activity; activity monitoring; monitoring systems; Astra Linux Special Edition

For citation: I.I. Andreev, S.O. Ivanov, T.N. Kopysheva, M.V. Nikandrov, T.N. Smirnova. Development of a mathematical model for assessing the quality of the implementation of a telemetry system into the organizational structure of the gas and smoke protection service. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(4):23-38. (In Russ) DOI:10.21822/2073-6185-2025-52-4-23-38.

Введение. Увеличение количества кибератак повышает риски утечки информации и компрометации автоматизированных рабочих мест в организациях и на предприятиях [1-3]. Поэтому мониторинг безопасности информации играет ключевую роль в своевременном обнаружении любой подозрительной активности в информационных системах. Подозрительная активность может быть признаком компьютерного инцидента, а один или несколько компьютерных инцидентов – кибератаки на защищаемую систему [4]. С учетом того, что большое количество кибератак происходит по причине ошибок, допущенных пользователями, возникает острая необходимость в непрерывном мониторинге необычной или отклоняющейся от нормы пользовательской активности [5-7].

Своевременное обнаружение компьютерных инцидентов позволяет реагировать на них гораздо быстрее, чем может быть осуществлена атака, что существенно повышает шансы на предотвращение кибератаки и минимизацию возможного ущерба от нее.

Мониторинг действий пользователей имеет важное значение для своевременного реагирования на инциденты информационной безопасности, предотвращения утечки конфиденциальной информации и негативных действий в информационной системе [8-10]. Его можно реализовать с помощью систем обнаружения вторжения – узловых и сетевых [11-13]. Такие меры позволяют увеличить количество информации для анализа событий безопасности и снизить вероятность обнаружения ложно-позитивного компьютерного инцидента в информационной системе [14, 15].

Учитывая тот факт, что государственные информационные системы (ГИС) и объекты критической информационной инфраструктуры (ОКИИ) [21] переходят на отечественные операционные системы согласно указам Президента № 166 [21] и № 250 [23], появляется необходимость разработки методов мониторинга нестандартной пользовательской активности в отечественной операционной системе специального назначения (ОССН). В качестве объекта исследования выбрана ОССН Astra Linux Special Edition. Актуальность объясняется следующими факторами:

- Уникальность направления. ОССН Astra Linux Special Edition [16] имеет встроенные средства защиты информации, каждое из которых работает независимо от других и подход к сбору событий от каждого из средств защиты информации уникален;
- Все больше предприятий, государственных органов и учреждений, а также компаний переходят на отечественные ОССН, например, Astra Linux Special Edition [17, 18].

В связи с этим возникает проблема – отсутствие специализированных инструментов для мониторинга ОССН. Данная проблема не решена, поскольку в условиях нестандартных конфигураций безопасности, которые предоставляет отечественная ОС специального назначения, использование открытых решений Wazuh и Open Search демонстрирует большое количество ложно-позитивных событий безопасности.

Поэтому появляется необходимость в глубокой адаптации стандартных правил корреляции, обнаружения и анализа событий под ОССН.

Постановка задачи. Для обнаружения нестандартной активности пользователей в ОССН необходимо комбинирование нескольких методов мониторинга.

- Подход с открытым исходным кодом. Использование систем мониторинга с открытым исходным кодом не только снижает затраты, но и обеспечивает масштабируемость и гибкость, следовательно, надежность.

- Профилактическая защита. Мониторинг необычной активности пользователей может помочь вовремя выявить потенциальные угрозы безопасности, утечки данных или попытки несанкционированного доступа [19, 20]. Такой подход имеет решающее значение для поддержания целостности и безопасности операционной системы и данных, которые она обрабатывает.

Цель работы: разработка и экспериментальная оценка метода интеграции и адаптации Open Source средств мониторинга для эффективного обнаружения аномальной пользовательской активности в операционной системе специального назначения Astra Linux Special Edition. Для достижения поставленной цели сформулированы следующие задачи:

1. Разработка архитектуры интегрированной системы мониторинга на базе open-source решений (Wazuh, Open Search) для сбора и корреляции событий безопасности в среде ОССН.

2. Адаптация и модификация стандартных правил корреляции, обнаружения и анализа событий (для audit.d, OSSEC, Suricata) под специфику встроенных механизмов защиты Astra Linux Special Edition (мандатный контроль, аудит Parsec) и интеграция с платформами анализа угроз (VirusTotal, URLhaus).

3. Экспериментальная оценка эффективности адаптированного решения по ключевым метрикам (процент обнаружения атак по MITRE ATT&CK, уровень ложных срабатываний, производительность) и анализ его соответствия требованиям стандартов (ГОСТ Р 59548-2022, NIST SP 800-92).

4. Методологическое обоснование подхода к адаптации open-source инструментов мониторинга под уникальные требования ОССН и формулирование практических рекомендаций.

Методы исследования. Методы мониторинга безопасности. Выбор методов мониторинга осуществлялся на основе следующих критериев, соответствующих требованиям ГОСТ Р 59548-2022[24] и NIST SP 800-92 [25]:

1. Полнота данных – инструмент должен собирать максимально полный набор событий.

2. Гибкость настройки – инструмент должен иметь возможность адаптировать правила корреляции и парсинга под особые механизмы ОССН (мандатный контроль и встроенные СЗИ).

3. Производительность – инструмент должен оказывать минимальное влияние на скорость и ресурсы ОС при сборе/обработке логов.

4. Поддержка стандартов – инструмент должен иметь совместимость с форматовыми спецификациями.

5. Масштабируемость – инструмент должен расти вместе с инфраструктурой.

Получать события безопасности системы можно как со встроенных средств, так и с помощью специального программного обеспечения, доступного в репозиториях операционной системы. Также можно использовать открытое программное обеспечение.

В результате проведения тестирования была составлена сравнительная характеристика вышеперечисленных способов (табл. 1).

В процессе сравнения было выявлено, что для формирования подробного журнала событий наилучшим образом подходит встроенное средство аудита – audit.d, хостовая система обнаружения вторжений ossec и сетевая система обнаружения вторжений suricata.

Таблица 1. Сравнительный анализ способов получения событий системы из Astra Linux Special Edition
Table 1. Comparative analysis of ways to get system events from Astra Linux Special Edition

Способ Method	Описание Description	Технические данные Technical data	Особенность Feature
С помощью встроенных средств Using built-in tools	С помощью файлов директории /var/log, а именно с помощью встроенных файлов журналов операционной системы Linux.	Журналы системы: auth.log или secure, secure.log, message.log или syslog.log, kern.log, cron.log, dpkg.log.	В данных журналах содержатся системные события
	С помощью утилиты syslog-ng, а именно получать события от другого узла, либо отправлять события на другой узел.	Осуществляется настройка конфигурационного файла syslog-ng.conf.	Можно получить данные от нескольких узлов и собрать их на одном узле, что значительно упрощает их анализ.
	С помощью циклического вызова команд Linux с определенной задержкой и записью вывода в файл.	Вызов следующих утилит: du, vmstat, w, htop, md5sum, audit.d, diff, users, last, lastlog, wtmp.	Можно получить данные, которых нет в журналах системы. Данные позволяют получать состояние использования ресурсов Linux.
С помощью программного обеспечения, доступного в репозиториях Using software available in repositories	С помощью утилиты аудита действий в операционной системе – audit.d.	Осуществляется наблюдение за директорией /etc/audit и файлов audit.log.	Позволяет отслеживать любые действия в системе, есть возможность настройки своих правил обнаружения.
	С помощью утилиты – межсетевого экранирования iptables.	Осуществляется наблюдение за журналом iptables.log.	Можно получить события о потенциальных атаках на узел, либо нелегитимное разрешение сетевых соединений.
	С помощью утилиты – межсетевого экранирования nftables	Осуществляется наблюдение за журналами nf_log, kern.log и syslog.	Позволяет получить более подробную информацию о сетевой активности, поддерживает механизмы IPv6, VLAN, MPLS и QoS.
С помощью открытого программного обеспечения Using open-source software	С помощью инструмента для сбора, парсинга и анализа логов – Logstash.	Осуществляется настройка конфигурационного файла logstash.yml. Так же конфигурацию можно задавать сразу в командной строке.	Может обрабатывать различные типы данных, логи и метрики, для быстрого и удобного парсинга есть GROK фильтры.
	С помощью сетевой системы обнаружения вторжений Suricata.	Осуществляется наблюдение за файлами /etc/suricata/rules/ suricata.yml eve.json	Позволяет отслеживать нелегитимные действия в контролируемой сети.
	С помощью узловой системы обнаружения вторжений Ossec.	Осуществляется настройка конфигурационного файла ossec.conf и наблюдение за журналом ossec.log.	Позволяет отслеживать действия в системе, есть возможность настройки своих правил обнаружения. В конфигурационный файл можно включить все вышеперечисленные способы.

На основе этих критериев были выбраны следующие инструменты:

1. audit.d - встроенное средство аудита Astra Linux Special Edition, которое обеспечивает полноту данных, гибкость настройки и минимальное влияние на производительность системы.

2. OSSEC - хостовая система обнаружения вторжений, которая предоставляет расширенные возможности анализа логов и обнаружения аномалий и интеграцию с audit.d для повышения детализации данных.

3. Suricata - сетевая система обнаружения вторжений, которая обладает высокой производительностью при анализе сетевого трафика и возможностью интеграции с OSSEC для комплексного мониторинга.

Комбинация audit.d, OSSEC и Suricata позволяет сформировать журнал событий, в котором отображены действия в системе на уровне хоста и сетевой активности, что делает выбранные инструменты оптимальным решением для мониторинга безопасности в операционной системе специального назначения.

Таким образом, для мониторинга нестандартной пользовательской активности подходят вышеописанные инструменты. Данные инструменты наиболее эффективно применять с системой мониторинга. Для анализа существующих открытых систем мониторинга Wazuh и Open Search составим таблицу анализа сведений о них (табл. 2).

Таблица 2. Таблица сравнений Wazuh OpenSearch
Table 2. Wazuh Open Search Comparison Table

Название Name	**Плюсы Pros**	**Минусы Cons**
Wazuh	Бесплатный SIEM и XDR с открытым исходным кодом. Множество готовых правил корреляции. Аудит конечных точек, отображение уязвимостей и оценка безопасности. Контроль целостности файлов и отслеживание изменений. Модуль MITRE ATT&CK для классификаций событий по тактикам и техникам. Агенты для отправки событий и аудита, а также для работы в режиме XDR. Взаимодействие с различными источниками информации, таких как IPS\IDS и межсетевые экраны. Индексатор на базе OpenSearch для записи данных в индексы. Возможность загружать и использовать все плагины OpenSearch.	Необходимость самостоятельной настройки и написания правил корреляции. Отсутствие быстрых обновлений правил детектирования угроз, необходимо обновлять каждый узел отдельно.
OpenSearch	Полностью основан на ELK, имеет открытый исходный код и легко масштабируется. Включает движок хранения и поиска, веб-интерфейс, среду визуализации данных и плагины. Каждый плагин способен работать отдельно от системы и их интегрировать с другими системами. Применяется для управления логами, сбора, систематизации и поиска данных.	Некоторые возможности, такие как машинное обучение и поддержка SQL, доступны только через плагины.

Выбор пал именно на них, так как они являются полностью открытыми системами, что позволяет проводить гибкую и быструю настройку, а также интеграцию с системами аудита и обнаружения вторжений. В качестве системы мониторинга был выбран Wazuh. Выбор Wazuh был осуществлен по следующим причинам:

1. Масштабируемость и гибкость. Открытая платформа для управления безопасностью и мониторинга событий, которая поддерживает интеграцию с множеством источников данных, включая журналы событий ОС, сетевые данные и другие специализированные решения. Удобство для мониторинга нестандартной активности в сложных инфраструктурах, где используются разные компоненты.

2. Интеграция с другими инструментами. Wazuh интегрируется с системами OSSEC, Suricata и Auditd, что позволяет централизовать сбор и анализ данных из разных источников. Например, OSSEC может собирать события с узлов, а затем передавать их в Wazuh для дальнейшего анализа и корреляции.

3. Поддержка правил и сигнатур. Включает обширную библиотеку предопределённых правил и возможностей создания собственных сигнатур для обнаружения аномалий. Это важно при мониторинге нестандартных действий, так как позволяет адаптироваться к специфическим сценариям использования.

4. Открытый исходный код. Использование инструментов с открытым исходным кодом снижает затраты и повышает прозрачность процессов обработки данных. Wazuh предоставляет возможность кастомизации и доработки под конкретные нужды организации без необходимости приобретения дорогостоящих лицензий.

5. Превентивные меры и оповещения. Способен автоматически реагировать на обнаружение подозрительных активностей, отправляя уведомления администраторам или инициируя защитные механизмы. Это позволяет оперативно реагировать на потенциальные угрозы до того, как они приведут к серьезным последствиям.

Таким образом, выбор Wazuh обусловлен его функциональностью, совместимостью с другими популярными инструментами безопасности и возможностью адаптации под уникальные требования системы мониторинга.

Условия, в которых проходила проверка работоспособности системы:

- мониторинг за работой системы в Wazuh;
- использование доступных инструментов в Wazuh;
- использование интеграции и скриптов Wazuh для получения эффективного результата в выявлении нестандартной активности пользователей;
- имитация действий пользователя для генерирования событий;
- применение доступных для пользователя инструментов и команд Linux;
- использование средств защиты информации в ОССН (мандатное управление доступом, мандатный контроль целостности, аудит parsec).

Для разработки правил audit.d и suricata был проведен анализ техник MITRE ATT&CK[26] с целью выявления возможного их применения в Astra Linux. Для работы сетевой системы обнаружения вторжения suricata были загружены правила с web-ресурса https://rules.emergingthreats.net/open/, проанализированы и адаптированы для анализа сетевой активности в Astra Linux Special Edition.

В качестве основы для правил audit.d (табл. 3), suricata (табл. 4) и ossec (табл. 5) использовались примеры из официальной документации. Каждый пример был тщательно проанализирован, и на его основе разрабатывались необходимые правила для мониторинга определенных действий пользователя в ОССН с учетом встроенных средств защиты информации. Каждое правило создавалось в соответствии с определенной техникой MITRE ATT&CK.

В табл. 3-5. представлены адаптированные правила.

Таблица 3. Audit.d-правила для отслеживания техник MITRE ATT&CK
Table 3. Audit.d-Rules for tracking MITRE ATT&CK Techniques

MITRE ID	**Описание действия** **Description of action**	**Правило audit.d** **Rule**
T1078.003	Создание/модификация локальных учётных записей	-w /usr/sbin/useradd -p x -k T1078_003 -w /usr/sbin/usermod -p x -k T1078_003 -w /usr/sbin/adduser -p x -k T1078_003
T1059.004	Выполнение shell-команд (bash, sh, sudo)	-a exit,always -F arch=b64 -S bash -k T1059.004 -a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=500 -k T1059.004
T1059.006	Запуск Python	-w /usr/bin/python -p x -k T1059.006 -w /usr/bin/python3 -p x -k T1059.006
T1053.003	Действия с crontab	-w /etc/crontab -p wa -k T1053.003 -a always,exit -F path=/usr/bin/crontab -F perm=x -k T1053.003
T1569	Управление сервисами	-w /usr/bin/systemctl -p x -k T1569 -w /usr/bin/systemd -p x -k T1569

Таблица 4. Suricata-правила для обнаружения техник MITRE ATT&CK
Table 4. Suricata-Rules for detecting MITRE ATT&CK Techniques

MITRE ID	Описание действия Description of action	Фрагмент правила Fragment of the rule
T1133	SSH-соединение на порт 22	alert ssh $EXTERNAL_NET any -> $HOME_NET 22 (msg:"Connect tp SSH"; ssh.software; content:"openssh"; sid:1000010;)
T1021.004	SSH-аутентификация	alert tcp $HOME_NET any -> any 22 (msg:"LOCAL SSH connect"; flow:established,to_server; app-layer-protocol:ssh; sid:1000008; rev:1;)
T1020	Эксфильтрация по SSH	alert tcp any any -> any 22 (msg:"Potential SSH exfiltration"; flow:es-tablished,to_server; app-layer-protocol:ssh; sid:1000011; rev:1;)

Таблица 5. Краткое описание разделов Wazuh Manager (ossec.conf)
Table 5. Brief description of the Wazuh Manager sections (ossec.conf)

Группа ID	Описание действия Description	Правила и условия Terms and Conditions
audit	Мониторинг выполнения команд	1 (Level 3): Audit: Command executed 2 (Level 12 → Parent:1): Audit: Suspicious command
perf	Контроль метрик системы	10 (Level 3): Metrics check 11 (Level 12 → Parent:10): cpu_usage_% >80% 12 (Level 12 → Parent:10): memory_usage_% >80%
malware	Обнаружение вредоносной активности	20 (Level 10): URL-угроза: url_threat=malware_download 21 (Level 15 → Parent:20): Malware activity detected

Обсуждение результатов. Система мониторинга пользовательской активности строится на основе руководства по мониторингу и анализу событий безопасности NIST SP 800-92 и приказа ФСБ №281. Однако были предложены решения для адаптации этих этапов к специфике операционной системы специального назначения и интеграции их с открытым программным обеспечением. Архитектура системы отображена на рис. 1.

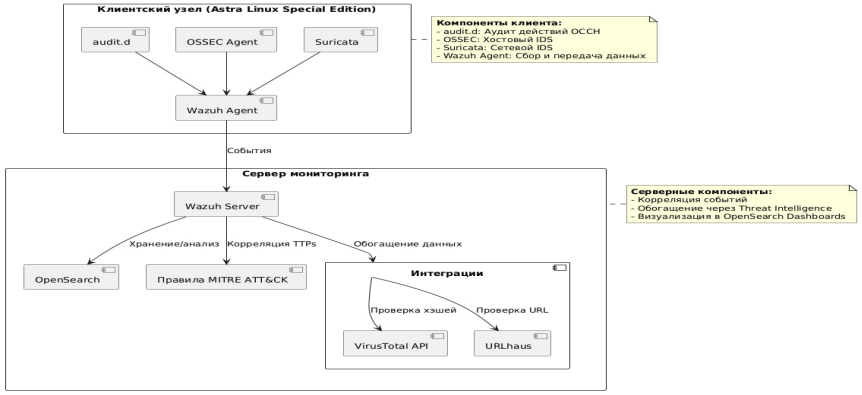

Рис. 1 – Архитектура системы
Fig. 1 – System architecture

Рассмотрим основные этапы обработки событий и способы реализации каждого компонента с помощью открытого программного обеспечения. Эти этапы описаны в NIST SP 800-92 [25] и в приказе ФСБ №281[27]. Этапы обработки событий:

- Сбор событий. Можно реализовать двумя способами: с агентом либо без агента (собирать данные через syslog-ng). Был реализован сбор событий с агентом.
- Нормализация событий – приведение необработанных событий в единый и читаемый формат. Реализуется с помощью декодеров и правил OSSEC.
- Агрегация событий. Реализуется с помощью Dashboards в Wazuh.
- Обогащение событий новыми данными для более точного анализа предупреждений системы мониторинга (обогащение сетевых событий, данных о хешах скачанных файлов и т.д.).
- Корреляция событий – анализ потока нормализированных событий и выделение из всего потока цепочки событий, которая свидетельствует о потенциальном

инциденте компьютерной безопасности. Применяются плагины корреляции OpenSearch, которые были интегрированы в Wazuh.

Метод анализа нестандартных действий пользователей в ОССН работает следующим образом:

1. Пользователь совершает действие в системе.
2. Создаются события в журналах системы.
3. Событие проходит вышеперечисленные этапы обработки событий.
4. Аналитик оценивает предупреждение в Wazuh.
5. В случае обнаружения подозрительной активности узел изолируется от сети.
6. Аналитик подключается к узлу и применяет меры по реагированию.
7. После устранения угрозы формируется новый пак правил на каждый узел.
8. После разработки пака правил он тестируется с помощью тестовых событий и цепочки атак.

Основные настройки конфигурационных файлов были взяты с официальных сайтов инструментов, проанализированы и адаптированы под ОССН. Для проверки работоспособности системы были смоделированы тестовые события для отдельных компонентов и цепочка атак, согласно MITRE ATT&CK, выполняемую из контролируемого узла для имитации нестандартной активности пользователя. Для тестирования работоспособности системы в целом была составлена цепочка атак из нескольких тактик и техник MITRE ATT&CK. Атака направлена на тестирование правил и системы мониторинга с целью выявления нестандартной активности пользователя, которая может указать на компрометацию учетных данных администратора или захват узла. Этапы атаки представлены ниже в таблице (табл. 6).

Таблица 6. Этапы атаки
Table 6. Stages of the attack

Техника Technique	**Описание действия Description of action**	**IOC**	**Критичность Criticality**
T1078.003	Вход в учётную запись пользователя с перехваченными данными	Новая запись в audit.log	Низкая Low
T1059.004	Использование Unix-shell для получения информации об узле	Вызов нетипичных команд: ip a, cat /etc/hosts, groups, systemctl status	Низкая Low
T1078.003	Вход в браузер под чужой учёткой и скачивание эксплойта	Обращение к подозрительным ссылкам	Средняя Medium
T1068	Эксплуатация уязвимости CVE-2024-1086 для получения прав root	Запуск скрипта с SHA256 d8dd09b01eb4e363d88ff53c0aace04c39dbea822b7adba7a883970abbf72a77, POC CVE-2024-1086	Высокая High
T1548.001	Закрепление в системе: правка sudoers, отключение пароля и создание нового админ-аккаунта	События useradd, правка sudoers, изменение /etc/shadow, запуск nano от системы и sudo от админа	Высокая High
T1070.003	Очистка истории команд терминала	Изменение хеша файла .bash_history	Низкая Low
T1003.008	Дамп учётных данных системы	Несанкционированное чтение /etc/passwd и /etc/shadow, первый sudo + чтение /etc/shadow	Высокая High
T1083	Перечисление файлов в директориях	Обращение к контролируемым каталогам неизвестным пользователем	Средняя Medium
T1595.001	Сканирование портов в подсети скриптом на Bash	Создание и запуск скрипта для сканирования #!/bin/bash for (i=1;i<255:i++) do echo > /dev/tcp/10.0.2.$i/24 && echo "Port is open" done	Высокая High
T1005	Сбор информации путем копирования файлов в один каталог	Копирование множества файлов в одну папку	Средняя Medium
T1020	Эксфильтрация данных по SSH	SSH-соединение к неизвестному узлу и передача файла	Высокая High
T1485	Удаление важных данных с узла	Удаление контролируемых файлов	Высокая High

В ходе тестирования работоспособности Suricata было зафиксировано нелегитимное сетевое обращение, выполнена загрузка вредоносного программного обеспечения с ресурса

https[:]//pastebin[.]com/raw/ZkwP7zPF (рис. 2). URLhaus: пометка {"found": 1} означает, что URL признан вредоносным. Правило Suricata 86601: «ET POLICY curl User-Agent Outbound» — срабатывает, когда видит исходящий HTTP-запрос с заголовком User-Agent = curl. Отчёт: https://urlhaus.abuse.ch/url/2045738/ показывает тип вредоносного ПО, когда и кем URL добавлен.

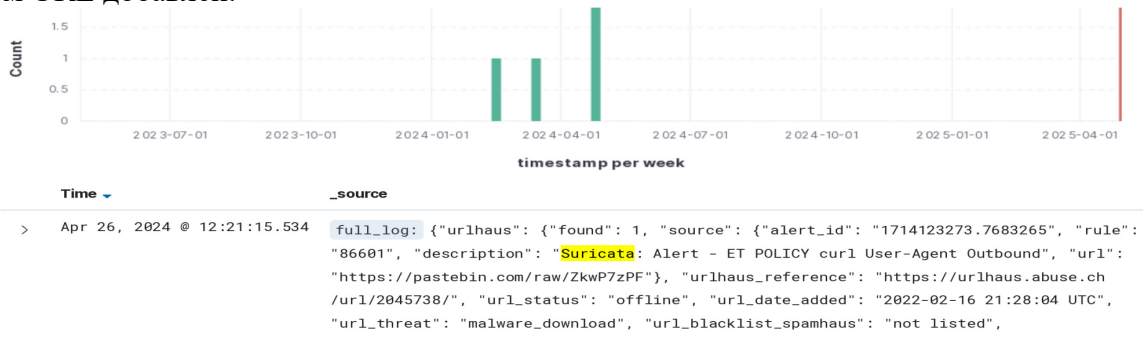

Рис. 2 – Тестирование сетевой системы обнаружения Suricata
Fig. 2 – Testing the Suricata Network detection system

В ходе тестирования работоспособности audit.d в системе было зафиксировано потенциально нелегитимное действие – передача файла с помощью scp (рис. 3). Запись фиксирует успешный запуск команды /usr/bin/scp от пользователя root, инициированный пользователем с auid=1000. Поскольку это соединение могло передавать файлы за пределы сервера, такая активность при отсутствии явной необходимости выглядит подозрительно и поэтому требует проверки.

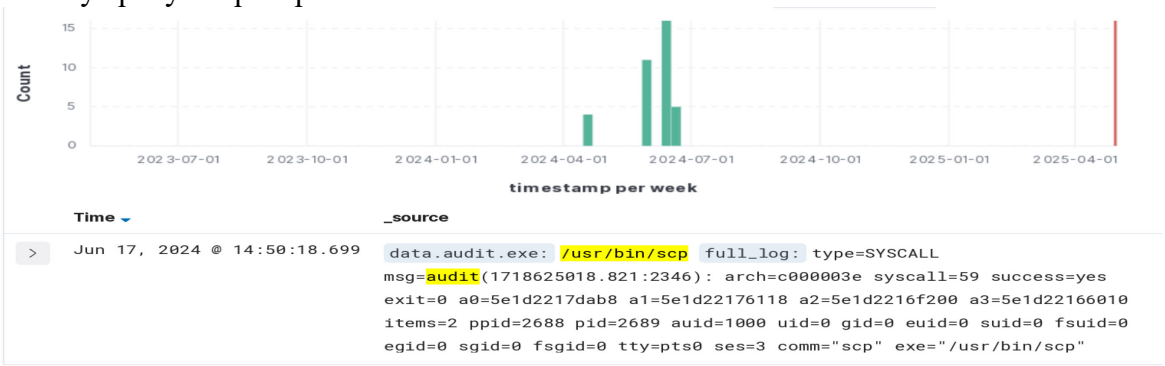

Рис. 3 – Тестирование аудита системы audit.d
Fig. 3 – Testing the audit of the audit.d system

С целью тестирования работоспособности правил OSSEC была выполнена проверка изменений файлов посредством модуля syscheck (рис. 4). Уведомление Wazuh о том, что файл был изменён: его размер вырос с 26625 до 26660 байт, изменился MD5-хеш, время модификации и содержимое, добавлена строка fly-wm [21:55:56] I: Locker finish.

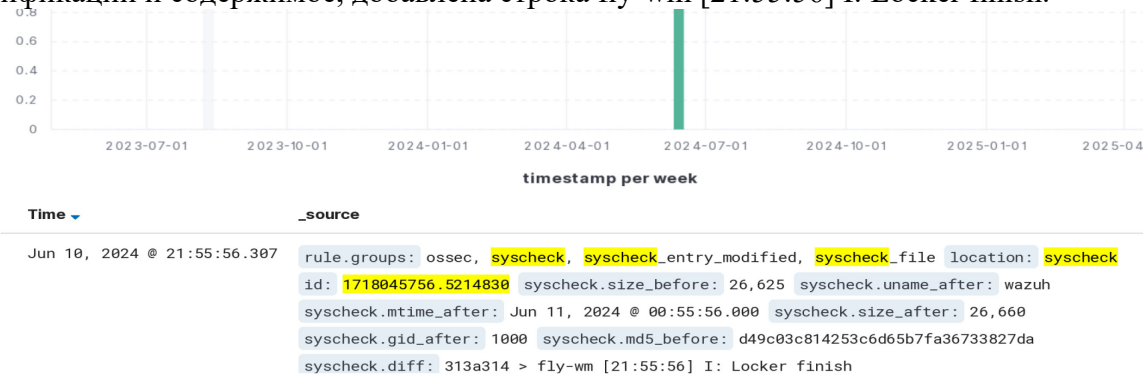

Рис. 4 – Тестирование узловой системы обнаружения вторжения OSSEC
Fig. 4 –Testing of the OSSEC Node Intrusion detection system

В ходе проведения исследований было сгенерировано общее количество событий: 586705 (сумма всех doc_count из JSON) (табл. 7). События аудита (audit, audit_command)

составляют 64.3% от общего числа, что указывает на активное использование механизмов контроля доступа и выполнения команд. Это главная область для мониторинга потенциальных угроз. Изменения в файловой системе (syscheck, syscheck_file, syscheck_entry_modified) занимают 99%. Все данные получены с Wazuh с помощью Dev Tools и HTTP запросов к серверу.

Таблица 7. События безопасности после тестирования
Table 7. Security events after testing

Категория Category	**Тип события Event Type**	**Количество Quantity**	**Доля (%) Share**
Аудит системы System audit	audit	200,691	34.2114%
	audit_command	176,532	30.0936%
	audit_configuration	21,470	3.6604%
	audit_selinux	2,480	0.4228%
	audit_anom	105	0.0179%
	audit_daemon	54	0.0092%
	audit_detections	41	0.0070%
Файловая система File System	syscheck	21,402	3.6484%
	syscheck_file	21,066	3.5911%
	syscheck_entry_modified	15,296	2.6073%
	syscheck_entry_added	5,116	0.8721%
	syscheck_entry_deleted	654	0.1115%
Безопасность Security	pam	3,308	0.5639%
	sudo	1,378	0.2349%
	rootcheck	430	0.0733%
	suricata	262	0.0447%
	ids	262	0.0447%
	virustotal	165	0.0281%
	vulnerability-detector	177	0.0302%
Системные ошибки System Errors	errors	14,481	2.4684%
	configuration_failure	5	0.0009%
Производительность Performance	performance_metric	7,186	1.2249%
Сетевая активность Network Activity	promisc	201	0.0343%
	usb	351	0.0598%
Агенты и мониторинг Agents and Monitoring	agent_flooding	108	0.0184%
	service_availability	116	0.0198%
	agent_restarting	5	0.0009%
Аутентификация Authentication	authentication_success	1,807	0.3081%
	authentication_failed	83	0.0141%
	invalid_login	2	0.0003%
Конфигурация ПО Software Configuration	dpkg	984	0.1677%
	config_changed	741	0.1263%
Системные процессы System Processes	ossec	22,410	3.8203%
	syslog	20,404	3.4784%
	systemd	29	0.0049%
	cron	2	0.0003%
	local	33	0.0056%
Веб-сервисы Web Services	web	12	0.0020%
	nginx	6	0.0010%
Дополнительные события Additional Events	chaos_malware_linux	895	0.1526%
	sca	262	0.0447%
	linuxkernel	211	0.0360%
	wazuh	113	0.0193%
	adduser	17	0.0029%
	attacks	6	0.0010%
	accesslog	6	0.0010%
	access_control	15	0.0026%
	su	6	0.0010%
	sshd	2	0.0003%

Для получения визуализации данных событий использовался Vega в Wazuh, а именно в OpenSearch Dashboard (рис. 5).

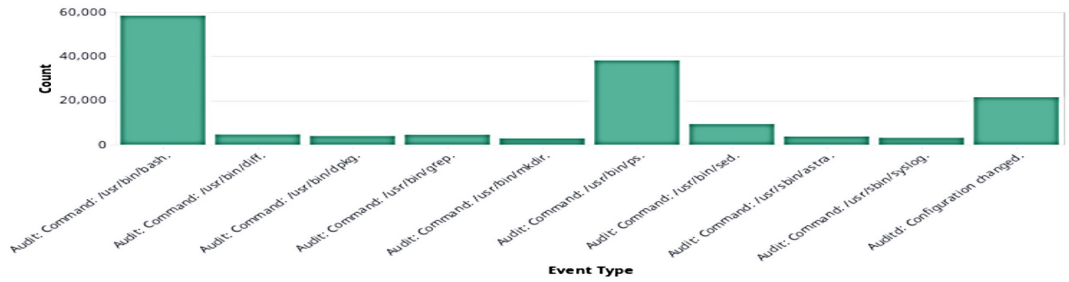

Рис. 5 – Результат исследований событий в системе мониторинга Wazuh
Fig. 5 – The result of research on events in the Wazuh monitoring system

Общее количество событий, классифицированных с помощью фреймворка для работы с MITRE ATT&CK – 21109 (табл. 8). Основную часть событий составляют две техники: T1565.001 (72.49%): Манипуляции с данными; T1078 (8.56%): Использование легитимных учетных записей для доступа.

Таблица 8. События по техникам MITRE ATT&CK
Table 8. MITRE ATT&CK Technical Events

Категория Category	**Техника (MITRE ATT&CK) Technique**	**Количество Quantity**	**Доля (%)Share**
Impact	T1565.001 (Stored Data Manipulation)	15,302	72.4895%
Privilege Escalation	T1548.003 (Sudo and Sudo Caching)	1,378	6.5270%
Defense Evasion	T1070.004 (File Deletion)	654	3.0975%
	T1485 (Data Destruction)	654	3.0975%
	T1562.001 (Disable Security Tools)	73	0.3458%
Initial Access	T1078 (Valid Accounts)	1,807	8.5601%
Execution	T1204.002 (Malicious File Execution)	895	4.2394%
Credential Access	T1203 (Exploitation for Credential Access)	22	0.1042%
Discovery	T1040 (Network Sniffing)	201	0.9521%
	T1057 (Process Discovery)	5	0.0237%
Lateral Movement	T1021.004 (SSH for Lateral Movement)	38	0.1800%
Credential Bruteforce	T1110.001 (Password Guessing)	62	0.2937%
Persistence	T1098 (Account Manipulation)	2	0.0095%
	T1136 (Create Account)	6	0.0284%
Другие	T1499 (Endpoint Denial of Service)	2	0.0095%
	T1531 (Account Access Removal)	2	0.0095%
	T1547.006 (Kernel Modules)	6	0.0284%

По умолчанию в Wazuh используются ossec со стандартными правилами, отслеживающие активность в системе: sca, auditd (selinux permission check), сессии pam, изменение состояния wazuh агента. По умолчанию suricata не установлена в Astra Linux Special Edition. После установки и загрузки необходимых правил, события сетевой системы обнаружения вторжений записываются в журнал eve.json (рис. 5).

Пример команды для получения информации о срабатывании правила «A Network Trojan was detected»: cat /var/log/suricata/eve.json | grep "A Network Trojan was detected" | tail -n 1 | jq -r '"\(.timestamp) \(.src_ip):\(.src_port) -> \(.dest_ip):\(.dest_port) [\(.alert.signature)]"'.

Вывод команды: 2024-12-01T15:51:27.029925+0300 10.0.2.4:55696 -> 77.88.44.242:80 [ET USER_AGENTS Suspicious User Agent (BlackSun)]. По умолчанию в Astra Linux Special Edition установлен auditd, он отслеживает только события parsec и syslog (рис. 6). Команда для получения правил auditd и их количества через терминал Linux: echo "$(for f in /etc/audit/rules.d/*.rules; do printf "%s:%d " "$(basename "$f")" "$(grep -cve '^\s*(#|$)' "$f")" done)$(grep -vE '^\s*(#|$)' /etc/audit/rules.d/audit.rules | tr '\n' ' ')". Вывод команды: 10-parsec.rules:4 astra-syslog.rules:36 audit.rules:18 github.rules:343 -b 8192 --backlog_wait_time 0 -f 1 -a exit,always -F arch=b64 -S kill -k kill_process -a exit,always -F arch=b64 -S exit_group -k kill_process. Проведенное тестирование цепочки атак, имитирующей действия злоумышленника по методике MITRE ATT&CK, позволило выявить ключевые уязвимости

в мониторинге ОССН Astra Linux. Каждый этап атаки (табл. 6) соответствует конкретным пробелам в обнаружении, которые были устранены за счет доработки правил audit.d, OSSEC и Suricata. Основные компоненты системы:

1. Система аудита. Основу составляет встроенный механизм аудита auditd, который отслеживает все события, происходящие в системе, включая доступ к файлам, выполнение команд, изменения прав доступа и другие важные операции.
2. Системы обнаружения вторжений.
3. Сетевой уровень. Для мониторинга сетевого трафика и выявления подозрительных действий была установлена и настроена система обнаружения вторжений Suricata. Система анализирует пакеты данных, проходящих через сеть, и сигнализирует об обнаружении потенциальных сетевых атак или попыток несанкционированного доступа к защищаемой сети.
4. Узловой уровень. На уровне отдельных хостов была внедрена узловая система обнаружения вторжений OSSEC. Эта система контролирует состояние файлов, процессы, лог-файлы и другую информацию на каждом узле сети, помогая обнаружить попытки реализации техник MITRE ATT&CK.

Интеграции и улучшения OSSEC: система OSSEC была улучшена за счет добавления интеграций с сервисами анализа вредоносных программ:

Virustotal – это позволило проводить автоматический анализ подозрительного контента и файлов, загружаемых в систему, на предмет наличия вредоносного программного обеспечения.

Urlhaus – данная интеграция помогает отслеживать запросы к известным вредоносным URL-адресам, блокируя потенциальные угрозы ещё до их реализации.

Выявленные слабые места:

Недостаточная детекция подозрительных событий. Для устранения этой слабости были добавлены правила auditd для отслеживания изменений в ключевых файлах и выполнения подозрительных команд и правила OSSEC для мониторинга изменений в файловой системе и логов. Часть добавленных правил audit.d выглядят так:

```
-w /etc/sudoers -p wa -k sudoers_changes
-w /etc/shadow -p wa -k shadow_changes
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/useradd -k user_creation
-a always,exit -F arch=b64 -S execve -F exe=/usr/bin/nano -k suspicious_editor
```

Часть добавленных правил OSSEC выглядят так:

```
<rule id="100001" level="7">
  <category>ossec</category>
  <decoded_as>syscheck</decoded_as>
  <description>Изменение в /etc/shadow</description>
  <group>system</group>
  <field name="file">/etc/shadow</field>
</rule>
```

Отсутствие корреляции событий. Для устранения этой слабости были добавлены правила корреляции, через интеграцию Wazuh с плагином корреляции из OpenSearch для анализа последовательности событий. Так же корреляцию событий можно реализовать через правила OSSEC, используемые в Wazuh. Именно этот способ реализован в виду его простоты. Пример добавляемого правила корреляции:

```
<group name="correlation,attack_chain,local">
  <rule id="200200" level="15" frequency="1" timeframe="600">
    <decoded_as>json</decoded_as>
    <field name="data.audit.exe">
/usr/sbin/useradd|/usr/sbin/usermod|/usr/sbin/adduser
    </field>
    <field name="data.audit.exe">
bash|ip a|cat /etc/hosts|groups|systemctl status
    </field>
    <field name="data.audit.exe">
```

```
d8dd09b01eb4e363d88ff53c0aace04c39dbea822b7adba7a883970abbf72a77
    </field>
    <field name="data.audit.exe">/usr/bin/nano|/usr/bin/sudo|useradd</field>
    <field name="data.audit.exe">/usr/bin/scp|\.bash_history</field>
    <description>
Корреляция многоэтапной атаки:
T1078.003 -> T1059.004 -> T1068 -> T1548.001 -> T1020/T1070.003
</description>
    <group>correlation,attack_chain,mitre</group>
  </rule>
</group>
```

Недостаточная реакция на IOC (Indicator of Compromise). Для устранения этой слабости были добавлены новые правила Suricata и OSSEC для отслеживания необходимых сетевых индикаторов компрометации из используемых техник MITRE ATT&CK. Пример добавляемого правила Suricata:

alert dns $HOME_NET any -> any any (msg: "IOC: DNS Query to Malicious FQDN"; dns.query; dataset:isset, domains_iocs, type string, load /etc/suricata/rules/domains_iocs.list, memcap 10mb, hashsize 1024; classtype: trojan-activity; sid:1000001; rev:1;) В файле /etc/suricata/rules/domains_iocs.list указаны URL адреса вредоносных доменов. Пример добавляемого правила OSSEC:

```
<group name="local,ioc,fim">
  <rule id="100700" level="15">
    <decoded_as>json</decoded_as>
    <field name="syscheck.md5_after">
d8dd09b01eb4e363d88ff53c0aace04c39dbea822b7adba7a883970abbf72a77
    </field>
    <description>IOC: Обнаружен файл с известным вредоносным SHA256-хешем</description>
    <group>syscheck,malware_ioc</group>
  </rule>
</group>
```

Конфигурации OSSEC, Suricata и Audit.d обеспечивают эффективное обнаружение и анализ подозрительной активности, описанной в цепочке атак. Выявленные уязвимости были устранены путем доработки правил и корреляции событий, что способствовало повышению общего уровня безопасности системы. Представлена лишь часть правил.

Предложенный подход позволяет обнаруживать критические этапы многоуровневых атак (T1068, T1548.001, T1020), что подтверждено тестированием цепочек MITRE ATT&CK (табл. 6). Единственный пропущенный этап — очистка истории команд (T1070.003), связан с ограничениями аудита bash-сессий. После адаптации правил доля ложных событий составила менее 0.03% от общего потока данных (табл. 7). Ложные события (audit_anom, audit_detections): 105 + 41 = 146. Доля ложных срабатываний: $\frac{146}{586705} * 100 = 0{,}025\%$. Это достигнуто за счет фильтрации шума, связанного с parsec и легитимными изменениями в системных файлах. Эффективность методики проверена на тестовых сценариях. «Базовые решения (Wazuh, OpenSearch) не учитывают специфику ОССН (например, события parsec), что приводит к ложным срабатываниям. Предложенная методика устранила этот недостаток за счет:

1. Адаптации 277 правил audit.d (табл. 3).
2. Введения 15 корреляционных правил OSSEC (табл. 5).
3. Интеграции с Suricata (табл. 4).

Автоматизация проверки через VirusTotal сократила время анализа для 100 событий категории chaos_malware_linux (895 случаев). Например, проверка хеша файла (рис. 2) с помощью URLhaus заняла менее 3 секунд. Полученные данные подтверждают, что адаптированные правила обеспечивают высокую эффективность обнаружения угроз (91,7%) и минимальный уровень ложных срабатываний (0,025%). Однако требуется развитие методов анализа для сложных многоэтапных атак.

$$\text{Эффективность} = \frac{\text{Обнаруженные этапы}}{\text{Всеэтапы}} * 100\% = \frac{11}{12} * 100\% = 91{,}7\%$$

В табл. 6 перечислено 12 этапов атаки, согласно техникам MITRE ATT&CK. Система обнаружила все этапы, кроме одного – T1070.003 (очистка истории команд).

Вывод. В работе предложен метод интеграции и адаптации open-source средств мониторинга (Wazuh, OSSEC, Suricata) для эффективного обнаружения аномальной пользовательской активности в ОС Astra Linux Special Edition. Это решает проблему отсутствия специализированных инструментов, совместимых со встроенными механизмами защиты ОССН (мандатным контролем, аудитом Parsec).

Предложенный метод основан на интеграции адаптированных правил audit.d, OSSEC и Suricata с платформой Wazuh, а также с VirusTotal и URLhaus, что обеспечивает соответствие требованиям NIST SP 800-92 и приказа ФСБ №281 за счет гибкой настройки под встроенные механизмы защиты, снижения ложных срабатываний, корреляции событий по тактикам MITRE ATT&CK. Архитектура протестирована в разных средах и соответствует ГОСТ Р 59548-2022.

Таким образом, работа вносит вклад в развитие методов мониторинга для отечественных операционных систем, имеет практическое значение для организаций, переходящих на ОССН, способствует снижению рисков компрометации за счет превентивного обнаружения аномалий, а также соответствует государственным стандартам безопасности.

Библиографический список:

1. Филимонова А.В., Заливина Д.А, Митрофанова Т. В. О социальной инженерии в кибербезопасности // Информационные технологии. Проблемы и решения, 2020. № 1 (10). С. 139-144.
2. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. 2025. Т. 4, № 1. С. 1001-1007.
3. Сафонова Е.Г., Егорова А.О., Маврин С.А. Вопрос актуальности проблемы целенаправленных кибератак на критическую информационную инфраструктуру // Энергетические установки и технологии. 2025. Т. 11, № 1. С. 110-116.
4. Создание собственного SOC при помощи классификации MITRE и opensource стека ELK / Степанов Я.В., Копышева Т.Н., Митрофанова Т.В. и др. // Информационные технологии в науке, управлении и образовании: междисциплинарный подход и тенденции развития: сб. матер. Всерос. науч.-практ. конф., 12 ноября 2021 года. Димитровград: Изд-во ДИТИ, 2021. С. 229-236.
5. Ермак К.К. Методы защиты от кибератак: современные подходы и технологии // Международный студенческий научный вестник. 2025. № 1. С. 4.
6. Аль-Кадхи М.А.А.А. Кибератаки: растущие угрозы, стратегии повышения осведомлённости и эффективные меры защиты // Актуальные исследования. 2025. № 7-1(242). С. 71-73.
7. Мукашев О. Методы защиты от распространенных типов кибератак // Интернаука. 2025. № 18-4(382). С. 65-68.
8. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. // Вопросы кибербезопасности, 2023. № 1 (53). С 13-27.
9. Нурьяров Р.Р. Современные методы и инструменты выявления целевых кибератак // Интернаука. 2025. № 12-1(376). С. 36-39.
10. Исакова Т.А. Безопасность информации: распределенная система обнаружения атак // Актуальные вопросы современной экономики. 2025. № 3. С. 596-600.
11. Нурьяров Р.Р. Архитектура SOC: повышение зрелости SOC для улучшения механизмов обнаружения и предотвращения кибератак // Интернаука. 2025. № 17-2(381). С. 5-16.
12. Порядок реагирования на наиболее популярные способы реализации кибератак в соответствии с техниками матрицы MITRE ATT&CK / Н.А. Николаев, А.Н. Вишнякова, И.В. Горбачев, О.М. Голембиовская //Информационная безопасность и защита персональных данных. Проблемы и пути их решения: сб. матер. и докл. XVI межрегион. науч.-практ. конф., Брянск, 29 апреля 2024 года. Брянск: Изд-во Брянск. техн. ун-та, 2024. С. 196-201.
13. Иванов А. С. Использование алгоритмов обработки естественного языка для идентификации техник из матрицы MITRE ATT&CK // Нанотехнологии. Информация. Радиотехника (НИР-24): Материалы Всерос. молодеж. науч.-практ. конф., Омск, 18 апреля 2024 года. Омск: Изд-во Омск. техн. ун-та, 2024. С. 68-71.
14. Zambianco M., Facchinetti C., Siracusa D. A Proactive Decoy Selection Scheme for Cyber Deception using MITRE ATT&CK // Computers & Security. 2025. Vol. 148. P. 104144.
15. Zhang Sh., Xue X. DeepOP: A Hybrid Framework for MITRE ATT&CK Sequence Prediction via Deep Learning and Ontology // Electronics. 2025. Vol. 14, No. 2. P. 257.
16. Головашов С., Агатий И. Подходы в обеспечении защиты информации при использовании Astra Linux Special Edition во встроенном оборудовании // Системный администратор. 2024. № 5(258). С. 26-41.
17. Зима В.М, Крюков Р.О. Подход к контролю действий привилегированных пользователей в критически важных автоматизированных системах // Вопросы оборонной техники. Серия 16: технические средства противодействия терроризму, 2021. С. 72-82.
18. Мылицын Р.Н, Девянин П.Н. Практика построения информационных систем в защищенном исполнении на базе операционной системы ASTRA LINUX SPECIAL EDITION // Состояние и перспективы развития современной

науки по направлению «Информационная безопасность». Сб. статей II Всероссийской научно-технической конференции. Т. 2. Анапа: Изд-во ФГАУ «Военный инновационный технополис "ЭРА"», 2020. С 448-453.
19. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions // Ömer Aslan, Semih Serkant Aktug, Merve Ozkan Okay, Abdullah Asım Yılmaz, Erdal Akin / March 2023 // Electronics 12(6):1-42 // DOI:10.3390/electronics12061333.
20. Review and insight on the behavioral aspects of cybersecurity // Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, Manish Kumar // April 2020 Cybersecurity 3(1) // DOI:10.1186/s42400-020-00050-w.
21. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации. Приказ ФСТЭК России N 239 от 25 декабря 2017 г.
22. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации. Указ Президента Российской Федерации от 30.03.2022 г. № 166.
23. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 01.05.2022 г. № 250.
24. ГОСТ Р 59548— 2022. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации.
25. Guide to Computer Security Log Management NIST SP 800-92
26. https://attack.mitre.org/matrices/enterprise/linux/ (дата обращения: 23.07.2025). Matrix Enterprise|MITRE ATT&CK [Электронный ресурс]: Linux Matrix.
27. Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации».

References:

1. Filimonova A.V., Zalivina D.A., Mitrofanova T.V. On Social Engineering in Cybersecurity. *Information Technologies. Problems and Solutions*. 2020; 1 (10): 139-144. (In Russ)
2. Nazaryan A.K., Kartsan I.N. Modern Cyberattacks: Classification and Protection Methods. *Informatics. Economics. Management.* 2025; 4; 1: 1001-1007. (In Russ)
3. Safonova E.G., Egorova A.O., Mavrin S.A. The relevance of the problem of targeted cyberattacks on critical information infrastructure*. Energy Plants and Technologies.* 2025; 11; 1: 110-116. (In Russ)
4. Creating your own SOC using the MITRE classification and the ELK opensource stack / Stepanov Y.V., Kopysheva T.N., Mitrofanova T.V., et al. // Information Technologies in Science, Management, and Education: An Interdisciplinary Approach and Development Trends: Collection of Materials. All-Russian Scientific and Practical Conference, November 12, 2021. Dimitrovgrad: Publishing House of DITI, 2021: 229-236. (In Russ)
5. Ermak K.K. Methods of protection against cyberattacks: modern approaches and technologies. *International student scientific bulletin*. 2025; 1: P. 4. (In Russ)
6. Al-Kadhi M.A.A.A. Cyberattacks: Growing Threats, Awareness-Raising Strategies, and Effective Protection Measures. *Current Research*. 2025; 7-1(242): 71-73. (In Russ)
7. Mukashev O. Methods of protection against common types of cyberattacks. *Internauka*. 2025;18-4(382):65-68 (In Russ)
8. The Subsystem of Computer Attacks Prevention on Critical Information Infrastructure Facilities: Analysis of Functioning and Implementation / Kotenko I.V., Saenko I.B., Zakharenko R.I., Velichko D.V. *Cybersecurity Issues*. 2023; 1 (53): 13-27. (In Russ)
9. Nur'yarov R.R. Modern Methods and Tools for Identifying Targeted Cyberattacks. *Internauka*. 2025; 12-1(376): 36-39. (In Russ)
10. Isakova T.A. Information Security: Distributed System for Detecting Attacks. *Actual Issues of Modern Economics*. 2025; 3: 596-600. (In Russ)
11. Nuryarov R.R. SOC Architecture: Enhancing SOC Maturity to Improve Cyber Attack Detection and Prevention Mechanisms. *Internauka*. 2025; 17-2(381): 5-16. (In Russ)
12. The procedure for responding to the most popular methods of implementing cyber attacks in accordance with the techniques of the MITRE ATT&CK matrix / N.A. Nikolayev, A.N. Vishnyakova, I.V. Gorbachev, O.M. Golembiovskaya // Information security and personal data protection. Problems and ways to solve them: collection of materials. and dokl. XVI interregion. Scientific and Practical conference, Bryansk, April 29, 2024. Bryansk: Publishing house Bryansk. tech. University, 2024: 196-201. (In Russ)
13. Ivanov A.S. The use of natural language processing algorithms to identify techniques from the MITRE ATT&CK matrix // Nanotechnology. Information. Radio engineering (NIR-24): Materials of the All-Russian Thank you. Scientific and Practical conference, Omsk, April 18, 2024. Omsk: Publishing house of Omsk. tech. University, 2024: 68-71. (In Russ)
14. Zambianco M., Facchinetti C., Siracusa D. A Proactive Decoy Selection Scheme for Cyber Deception using MITRE ATT&CK. *Computers & Security*. 2025; 148: 104144.
15. Zhang Sh., Xue X. DeepOP: A Hybrid Framework for MITRE ATT&CK Sequence Prediction via Deep Learning and Ontology. *Electronics*. 2025; 14; 2: P. 257.
16. Golovashov S., Agatiy I. Approaches to Ensuring Information Security When Using Astra Linux Special Edition in Embedded Equipment. *System Administrator*. 2024; 5(258): 26-41. (In Russ)
17. Zima V.M., Kryukov R.O. Approach to Controlling the Actions of Privileged Users in Critical Automated Systems*. Issues of Defense Technology*. Series 16: Technical Means of Countering Terrorism, 2021: 72-82. (In Russ)
18. Mylitsyn R.N., Devyanin P.N. The Practice of Building Information Systems in a Protected Design Based on the ASTRA LINUX SPECIAL EDITION Operating System // The State and Prospects of Modern Science Development in the Field of Information Security. Collection of Articles from the II All-Russian Scientific and Technical Conference. Vol. 2. Anapa: Military Innovative Technopolis ERA, 2020: 448-453. (In Russ)

19. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions // Ömer Aslan, Semih Serkant Aktug, Merve Ozkan Okay, Ab-dullah Asım Yılmaz, Erdal Akin / March 2023 // Electronics 12(6):1-42 // DOI:10.3390/electronics12061333.
20. Review and insight on the behavioral aspects of cybersecurity // Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, Manish Kumar / April 2020 // Cyber-security 3(1) // DOI:10.1186/s42400-020-00050-w.
21. On Approval of Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation. Order of the FSTEC of Russia No. 239 of December 25, 2017. (In Russ)
22. On Measures to Ensure the Technological Independence and Security of the Critical Information Infrastructure of the Russian Federation. Decree of the President of the Russian Federation No. 166 of March 30, 2022. (In Russ)
23. On Additional Measures to Ensure the Information Security of the Russian Federation. Decree of the President of the Russian Federation No. 250 of May 1, 2022. (In Russ)
24. GOST R 59548-2022. Information Protection. Registration of Security Events. Requirements for Registered Information. (In Russ)
25. Guide to Computer Security Log Management NIST SP 800-92.
26. https://attack.mitre.org/matrices/enterprise/linux/ (accessed July 23, 2025). Matrix Enterprise|MITRE ATT&CK [Electronic resource]: Linux Matrix.
27. Order of the FSB of Russia dated June 19, 2019 No. 281 "On approval of the Procedure, technical conditions for the installation and operation of tools designed to detect, prevent, and eliminate the consequences of computer attacks and respond to computer incidents, with the exception of tools designed to search for signs of computer attacks in telecommunication networks used to organize the interaction of critical information infrastructure facilities of the Russian Federation" (In Russ)

Сведения об авторах:

Андреев Илья Игоревич, аспирант кафедры математического и аппаратного обеспечения информационных систем; andreev054@mail.ru; ORCID: 0000-0004-7624-5829.

Иванов Сергей Олегович, старший преподаватель кафедры математического и аппаратного обеспечения информационных систем; v101-11@mail.ru; ORCID: 0000-0003-3918-3919.

Копышева Татьяна Николаевна. кандидат физико-математических наук, доцент, заведующий кафедрой математического и аппаратного обеспечения информационных систем; tn_pavlova@mail.ru; ORCID: 0000-0003-3392-1431.

Никандров Максим Валерьевич, кандидат технических наук, директор ООО «Интеллектуальные сети», nikandrov@igrids.ru; ORCID: 0000-0001-6846-3384.

Смирнова Татьяна Николаевна, кандидат физико-математических наук, доцент, доцент кафедры математического и аппаратного обеспечения информационных систем; smirnova-tanechka@yandex.ru; ORCID: 0000-0001-6687-9415.

Information about the authors:

Ilya I. Andreev, Graduate Student, Department of Mathematical and Hardware Support of Information Systems, andreev054@mail.ru; ORCID: 0000-0004-7624-5829.

Sergey O. Ivanov, Senior Lecturer, Department of Mathematical and Hardware Support of Information Systems, v101-11@mail.ru; ORCID: 0000-0003-3918-3919.

Tatyana N. Kopysheva, Cand. Sci. (Physical and Mathematical), Assoc. Prof., Head of the Department of Mathematical and Hardware Support of Information Systems, tn_pavlova@mail.ru; ORCID: 0000-0003-0935-0384.

Maksim V. Nikandrov, Cand. Sci. (Eng.), Director of Intelligent Networks LLC, nikandrov@igrids.ru; ORCID: 0000-0001-6846-3384.

Tatiana N. Smirnova, Cand. Sci. (Physical and Mathematical), Assoc. Prof., Assoc. Prof., Department of Mathematical and Hardware Support of Information Systems, smirnova-tanechka@yandex.ru; ORCID: 0000-0001-6687-9415.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 23.07.2025.

Одобрена после рецензирования/Reviced 11.09.2025.

Принята в печать/Accepted for publication 30.10.2025.