УДК 004.05 **DOI: 10.18413/2518-1092-2024-9-2-0-5**

Надейкина В.С.
Маслова М.А.

АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЯ С ОТКРЫТЫМ КОДОМ ДЛЯ ИНТЕГРАЦИИ С ОТЕЧЕСТВЕННЫМИ ОПЕРАЦИОННЫМИ СИСТЕМАМИ

Севастопольский государственный университет,
ул. Университетская, 33, г. Севастополь, 299053, Россия

e-mail: nice.nadeykina@mail.ru, mashechka-81@mail.ru

Аннотация
В статье были рассмотрены такие IDS/IPS как Snort, Suricata, Fail2Ban и OSSEC, имеющие открытый исходный код. Проанализированы их механизмы обеспечения сетевой безопасности, включая архитектуру, функции, инструменты и реализуемые задачи. Рассмотрена возможность интеграции этих систем с отечественными операционными системами. В заключении подчеркивается, что IDS/IPS являются лишь одним из многих слоев защиты, которые должны быть внедрены для эффективного обеспечения безопасности. Только комплексный подход к безопасности может являться ключом к защите от современных киберугроз.
Ключевые слова: системы обнаружения вторжений; системы предотвращения вторжений; IDS; IPS; отечественные операционные системы; ОС; программные продукты; оценка безопасности; открытый исходный код
Для цитирования: Надейкина В.С., Маслова М.А. Анализ систем обнаружения и предотвращения вторжения с открытым кодом для интеграции с отечественными операционными системами // Научный результат. Информационные технологии. – Т.9, №2, 2024. – С. 41-48. DOI: 10.18413/2518-1092-2024-9-2-0-5

Nadeykina V.S.
Maslova M.A.

ANALYSIS OF OPEN-SOURCE INTRUSION DETECTION AND PREVENTION SYSTEMS FOR INTEGRATION WITH RUSSIAN OPERATING SYSTEMS

Sevastopol State University,
33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: nice.nadeykina@mail.ru, mashechka-81@mail.ru

Abstract
The article reviewed IDS/IPS such as Snort, Suricata, Fail2Ban and OSSEC, which have open-source code. Their mechanisms for ensuring network security, including architecture, functions, tools and implemented tasks, are analyzed. The possibility of integrating these systems with Russian operating systems is considered. In conclusion, it is emphasized that IDS/IPS are just one of the many layers of protection that must be implemented to ensure effective security. Only an integrated approach to security can be the key to protecting against modern cyber threats.
Keywords: intrusion detection systems; intrusion prevention systems; IDS; IPS; Russian operating systems; OS; software products; security assessment; open-source
For citation: Nadeykina V.S., Maslova M.A. Analysis of open-source intrusion detection and prevention systems for integration with russian operating systems // Research result. Information technologies. – T.9, №2, 2024. – P. 41-48. DOI: 10.18413/2518-1092-2024-9-2-0-5

ВВЕДЕНИЕ

В современном мире, где киберпреступность постоянно развивается, а методы кибератак становятся все более изощренными, наблюдается постоянный рост количества инцидентов безопасности.

По оценке Positive Technologies во II квартале 2023 года количество инцидентов увеличилось на 4% по сравнению с предыдущим кварталом и выросло на 17% относительно II квартала 2022. При этом доля атак на компьютеры, серверы и сетевое оборудование в организациях составляет 90%. В настоящее время самым распространенным методом атак (64%) является использование шифровальщиков (ransomware) [1]. Ввиду этого возникает необходимость повышения мер безопасности, в том числе безопасности сетей.

Одним из инструментов обеспечения безопасности сетей выступают системы обнаружения и предотвращения вторжений (IDS/IPS). Такие системы служат «первой линией обороны», обнаруживают и блокируют несанкционированные действия прежде, чем они смогут нанести критических ущерб.

Программы с открытым исходным кодом позволяют пользователям настраивать и модифицировать программное обеспечение в соответствии с их потребностями. Существует множество IDS/IPS с открытым исходным кодом, каждая из которых имеет свои сильные и слабые стороны. Понимание процессов функционирования различных IDS/IPS помогут компаниям выбрать подходящую систему для защиты их бизнеса.

В соответствии с новыми требованиями российского законодательства компании активно переходят на отечественное программное обеспечение. Ввиду этого актуально рассмотреть возможность интеграции IDS/IPS с открытым исходным кодом с отечественными операционными системами.

ОСНОВНАЯ ЧАСТЬ

Система обнаружения вторжений (Intrusion Detection System, IDS) и система предотвращения вторжений (Intrusion Prevention System, IPS) используются для защиты от сетевых атак. IDS в основном используются для обнаружения угроз или вторжений в сегмент сети. Однако IPS сосредоточены на идентификации этих угроз или вторжений для блокирования или прекращения их активности.

IDS развертываются вне диапазона в сети, что означает, что весь сетевой трафик передается в эту систему, но не через промежуточные устройства, возможности обработки соответствуют средней загрузке сети. IPS развертываются встроенными в сеть средствами, они проходят между устройствами и работают при пиковой нагрузке на сеть с большими буферами памяти для поглощения пакетов трафика, что неприемлемо. IDS и IPS могут регистрировать ложные срабатывания, однако при этом IPS может заблокировать законный трафик [2].

Рассмотрим существующие решения систем обнаружения и предотвращения вторжений (IDS/IPS).

Snort — это сетевая IDS с открытым исходным кодом для глубокого контроля сетевого потока.

Механизм обработки пакетов состоит из следующих этапов [4]:

1) Сбор трафика из действующей сети или файла pcap;

2) Расшифровка пакетов с использованием процедур идентификации структуры пакетов для протоколов канального уровня и портов;

3) Прохождение пакетами ряда этапов предварительной обработки, где на каждом этапе проверяется тип полученного пакета и его «поведение»;

4) Проверка пакетов на соответствие правилам механизмом обнаружения, регистрация и обработка несоответствий.

Архитектура обработки пакетов Snort отображена на рисунке 1.

Рис. 1. Архитектура обработки пакетов Snort
Fig. 1. Snort`s Packet Processing Architecture

Правила Snort состоят из двух основных разделов: заголовка правила и тела правила. Заголовок правила определяет действие, которое следует предпринять при совпадении трафика, а также протоколы, сетевые адреса, номера портов и направление трафика, к которым должно применяться правило. При написании тела правила играют роль критерии полезной нагрузки и неполезной нагрузки, которые должны соблюдаться для совпадения этого правила.

Устанавливая сетевой интерфейс хоста в «неразборчивый» режим (Promiscuous Mode), можно использовать Snort как сниффер пакетов. Это позволит проводить мониторинг всего объема сетевого трафика на локальном сетевом интерфейсе. Отслеживаемый трафик отображается в консоли.

Стоит отметить, что Snort не имеет графической оболочки (GUI), поэтому вся работа с программой может выполняться только через командную строку.

Suricata заимствует много функциональности у Snort, однако в ней реализованы некоторые отличные функции.

Suricata – программа с открытым исходным кодом, которая может функционировать как IDS, IPS, монитор сетевой безопасности или регистратор pcap [6]. Она имеет механизм масштабируемого потока, механизм потоковой передачи TCP, механизм дефрагментации IP и анализирует протоколы на канальном и прикладном уровнях. Она также имеет анализатор HTTP с отслеживанием состояния, который регистрирует транзакции и может извлекать файлы. Механизм обнаружения Suricata очень мощный, высокоэффективный, конфигурируемый и имеет гибкие настройки для конкретных потребностей.

Гибкие настройки многопоточных возможностей Suricata позволяют настроить запускать от одного потока вплоть до десятков, а также назначать потоки определенным процессорам или распределять их по всем доступным процессорам в системе.

Suricata имеет четыре модуля потоков для обработки пакетов [4]:

1) Модуль сбора пакетов собирает пакеты из сети или из файла pcap;

2) Декодирование и модуль прикладного уровня Stream декодирует пакеты на основе их протоколов и портов, выполняет отслеживание потока, где проверяет правильность сетевого подключения, восстанавливает исходный поток пакетов и проверяет прикладной уровень;

3) Модуль обнаружения может иметь несколько потоков обнаружения, запущенных одновременно, он сравнивает трафик с установленными правилами;

4) В последнем модуле на основе правил выполняются действия и регистрируются события.

Схема многопоточной архитектуры обнаружения отображена на рисунке 2.

Рис. 2. Многопоточная архитектура обнаружения Suricata
Fig. 2. Suricata`s Multithreaded Architecture

Для обнаружения вредоносного трафика Suricata использует систему правил подобную Snort. Различие заключаются в том, что Suricata использует собственный инструмент для упрощения управления и обновления наборов правил.

У Suricata также как у Snort нет графической оболочки.

Обе выше проанализированные программы интегрируются с такими отечественными операционными системами как Astra Linux, ALT Linux и ROSA Linux.

Fail2Ban — это IPS с открытым исходным кодом, которая помогает обеспечить защиту сервера от несанкционированных попыток входа в систему и атак методом перебора (брутфорс). Может работать на POSIX-системах, имеющих встроенный менеджер пакетов и брандмауэр (например, iptables).

О признаках несанкционированных попыток входа в систему можно судить, проанализировав системные журналы (логи). К таким признакам могу относиться регулярные попытки подключения с разных IP-адресов, запросы к различным портам сервера, запросы на те или иные ресурсы.

Fail2Ban сканирует логи для обнаружения неудачных попыток входа в систему и автоматически создает новые правила брандмауэра, блокирующие IP-адрес источника, который пытался войти в систему. Интервал времени блокирования определяется настройкой правил (фильтров).

Фильтры представляют собой набор регулярных выражений для поиска ключевых слов в файлах логов. В стандартной конфигурации Fail2Ban встроены некоторые фильтры, например, sshd, который отслеживает файлы журналов SSH и блокирует IP-адреса, которые совершают слишком много неудачных попыток входа, однако можно самостоятельно писать и настраивать фильтры, которые будет отслеживать конкретные паттерны в поведении злоумышленников и блокировать их попытки проникновения на сервер.

Fail2Ban сканирует системные журналы для обнаружения неудачных попыток входа в систему и автоматически создает новые правила брандмауэра для блокировки IP-адреса источника, который пытался войти в систему. Временной интервал для блокировки определяется настройками правил.

Принцип работы File2Ban схематично отображен на рисунке 3.

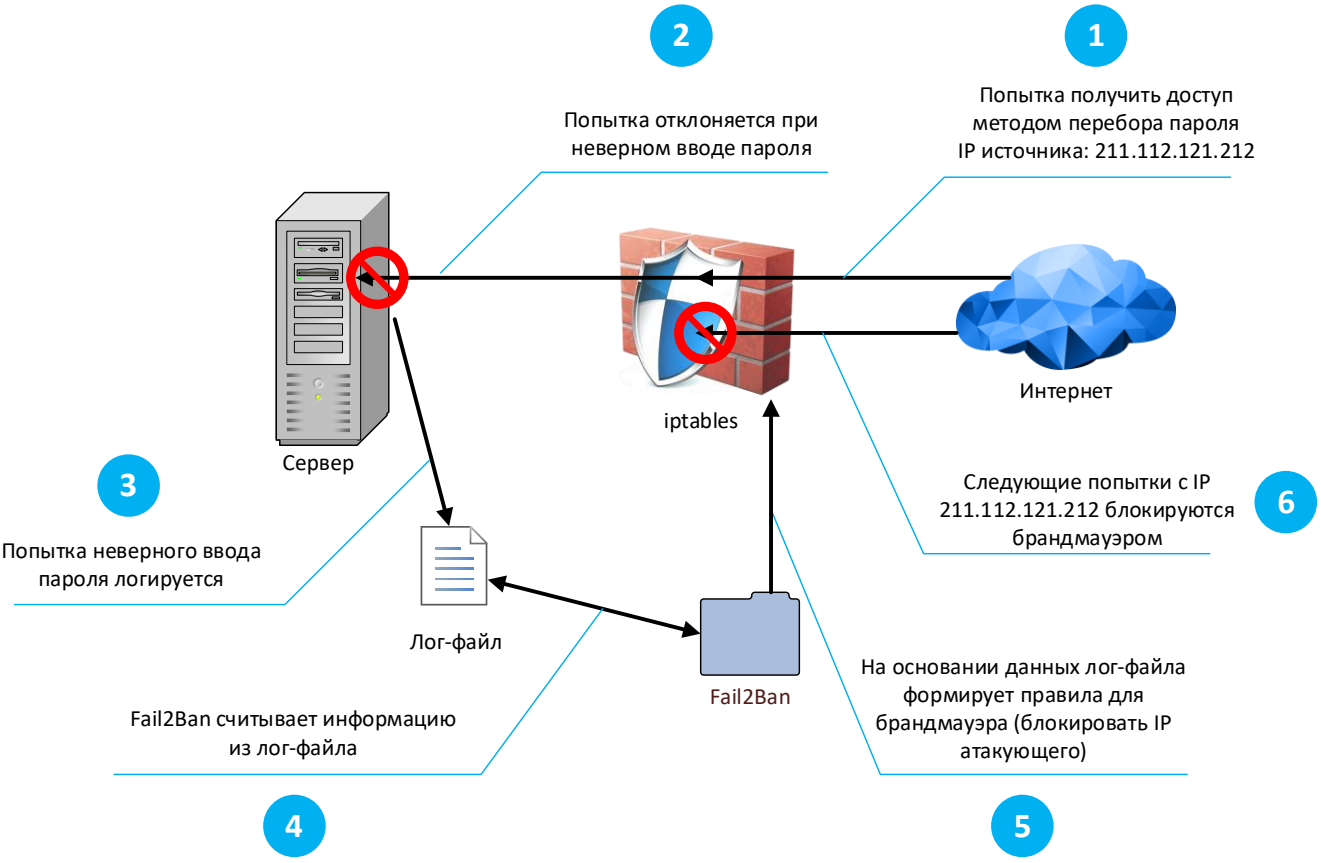

Рис. 3. Принцип работы Fail2Ban
Fig. 3. How Fail2Ban works

У Fail2Ban довольно низкие системные требования. При конфигурации только с sshd и несколькими различными правилами, Fail2Ban требует около 500 Мб памяти и загружает 1 ядро CPU в среднем менее чем на 0,2% [8].

Интегрируется с операционными системами семейства Debian (Astra Linux).

OSSEC — это хостовая IDS (HIDS) с открытым исходным кодом.

Опишем подробнее ее функционал.

OSSEC осуществляет сбор и анализ журналов событий, а также формирует уведомление о подозрительных действиях (например, сбой аутентификации, установка пакета или повышение привилегий пользователя). Действия, которые будут считаться подозрительными описываются администратором в правилах.

Частыми целями хакерских атак являются модификация, удаление или добавление данных путем воздействия на файлы и каталоги. OSSEC выполняет регулярные проверки целостности файлов и каталогов (syscheck) и отправляет информацию о контрольной сумме на сервер. Таким

образом, попытки атак на файловую систему можно будет выявить путем сравнения контрольных сумм.

Поведение хакеров при атаках характеризуется попытками скрытия, фальсификации или удаления данных о своих действиях в журналах безопасности. OSSEC использует файлы базы данных, содержащие в себе информацию о различных вредоносных программах. На основании этих данных OSSEC может обнаруживать действия, выполняемые с помощью внедрения вредоносного ПО.

Функция активного реагирования на определенные действия реализуется с помощью предварительно настроенных сценариев, которые будут запущены в случае обнаружения подозрительных действий в системе. Это мощная функция, которую можно творчески использовать для снижения мощности различных типов атак и потенциальных рисков.

Все описанные функции позволяют реализовывать «агенты» или другие методы. Агенты и менеджеры – части архитектуры OSSEC. Агент представляет собой очень маленький пакет, работающий в собственной изолированной среде и оказывающий очень незначительное влияние на производительность системы. Менеджер централизованно собирает всю информацию, полученную от агентов и других устройств, отслеживаемых другими методами, и хранит ее для облегчения администрирования всей системы. Связь менеджеров и агентов осуществляется через порт 1514 UDP/TCP, который используется для основной связи, и порт 1515, который используется только для отправки запроса на регистрацию менеджеру [9]. Такое архитектурно решение подходит для небольших компаний, для которых не характерна обработка больших объемов информации. Для больших компаний, которые нуждаются в обработке большого количества событий, можно развернуть OSSEC в режиме кластера. При таком архитектурном подходе количество агентов и менеджеров увеличивается, тем самым обеспечивая распределение нагрузки.

OSSEC имеет «ELK Stack», который включает в себя такие инструменты как Elastic Search, Logstash и Kibana. Рассмотрим подробнее каждый инструмент.

Elastic Search – это поисковая система, которая может хранить большие объемы данных и добавлять такие функции, как поиск, фильтры и другие расширенные функции поиска. Этот инструмент используется для поиска по агрегированным журналам, отправляемыми агентами. Каждый фрагмент данных, проиндексированный в Elastic Search, называется «документом». Если индекс содержит слишком много данных и занимает слишком много места на одном узле, то он может быть разделен на «сегменты», которые тоже являются индексами. Сегментация используется для повышения производительности, обеспечивая гибкость распределения данных по нескольким узлам.

Kibana представляет собой браузерную программу и используется для добавления визуального интерфейса ко всем другим инструментам, что облегчает процесс просмотра журналов и других конфигураций. Запускается через порт 5601 и питается от Node.js.

Logstash, представляет собой механизм анализа данных, работающий в соответствии с правилами получения, анализа, индексации и передачи журналов в Elastic Search [10].

Интеграционная архитектура OSSEC отображена на рисунке 4.

OSSEC имеет возможность интеграции с Astra Linux, ALT Linux и ROSA Linux.

Выбор системы обнаружения и (или) предотвращения вторжения зависит от конкретных задач. Например, Snort или Suricata могут быть лучшим выбором для мониторинга сетевого трафика, в то время как Fail2Ban или OSSEC могут быть более подходящими для защиты от атак на уровне хоста [11].

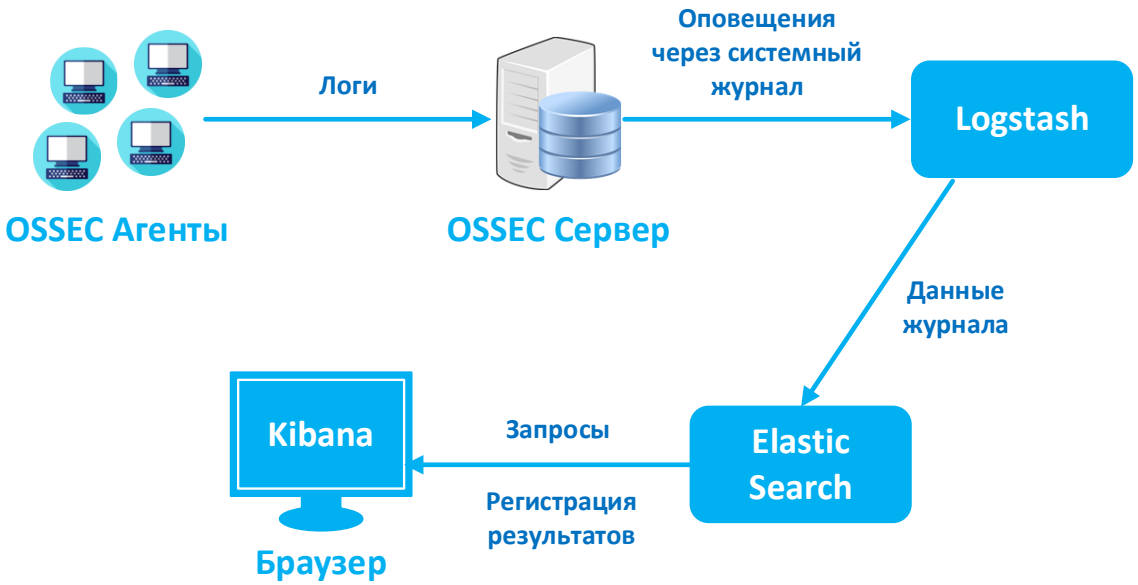

Рис. 4. Интеграционная архитектура OSSEC
Fig. 4. Integration architecture of OSSEC

ЗАКЛЮЧЕНИЕ

При постоянном росте количества инцидентов безопасности ввиду развития уровня киберпреступности, компаниям необходимо повышать меры безопасности своих информационных ресурсов.

Для обеспечения сетевой безопасности широко используются системы обнаружения и предотвращения вторжений (IDS/IPS).

В статье были рассмотрены такие IDS/IPS как Snort, Suricata, Fail2Ban и OSSEC, имеющие открытый исходный код.

Все рассмотренные системы имеют возможность интеграции с такими отечественными операционными системами как Astra Linux, ALT Linux и ROSA Linux.

Каждая система имеет уникальные преимущества реализации механизмов защиты. Разницы архитектур, функций и инструментов являются важными аспектами при выборе конкретной системы для обеспечения сетевой безопасности бизнеса.

Однако, несмотря на все преимущества IDS/IPS, важно помнить, что они являются лишь одним из многих слоев защиты, которые должны быть внедрены для эффективного обеспечения безопасности. Только комплексный подход к безопасности может являться ключом к защите от современных киберугроз [12].

Список литературы

1. Актуальные киберугрозы: II квартал 2023 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/
2. Ashoor A.S., Gore S. Intrusion detection system (IDS) & intrusion prevention system (IPS): Case study // International Journal of Scientific & Engineering Research. – 2012. – T. 2. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ddcb13f5dc671786b6fef5aa1fc4cc0285c4c79d
3. Snort – Network Instruction Detection. URL: https://www.snort.org/
4. Hoover C. Comparative study of snort 3 and suricata intrusion detection systems. – 2022. URL: https://scholarworks.uark.edu/csceuht/105/
5. Home – Suricata. URL: https://suricata.io/
6. Форд М. и др. Процесс передачи данных Fail2ban в адаптивную корпоративную систему обнаружения и предотвращения вторжений // SoutheastCon 2016. – IEEE, 2016. – С. 1-4. URL: https://iocscience.org/ejournal/index.php/mantik/article/view/673/434
7. Как защитить SSH с помощью Fail2Ban. Руководство для начинающих. URL: https://itshaman.ru/articles/3016/kak-zashchitit-ssh-s-pomoshchyu-fail2ban-rukovodstvo-dlya-nachinayushchikh

8. Безопасность сетевых соединений. URL: https://maximalisimus.github.io/Articles/The-security-of-network-connections.html#part5.0

9. OSSEC – World`s Most Widely Used Host Intrusion Detected System – HIDS. URL: https://www.ossec.net/

10.Teixeira D. et al. OSSEC IDS extension to improve log analysis and override false positive or negative detections //Journal of Sensor and Actuator Networks. – 2019. – Т. 8. – №. 3. – С. 46. URL: https://www.mdpi.com/2224-2708/8/3/46.

11.Пилькевич П.В., Маслова М.А. Влияние индексов реляционных баз данных на производительность поиска // Угрозы и риски на Юге России в условиях геополитического кризиса. Достижения и перспективы научных исследований молодых ученых Юга России: Материалы научных мероприятий: Всероссийской конференции с международным участием; XIX Ежегодной молодежной научной конференции, Ростов-на-Дону, 15– 29 марта 2023 года. – Ростов-на-Дону: Федеральное государственное бюджетное учреждение науки "Федеральный исследовательский центр Южный научный центр Российской академии наук", 2023. – С. 310.

12.Реализация ESG-принципов в стратегии устойчивого развития экономики России / Н.Г. Вовченко, Н.Г. Кузнецов, Е.Н. Макаренко [и др.]. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – 508 с.

References

1. Current cyber threats: The second quarter of 2023. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/

2. Ashoor A.S., Gore S. Intrusion detection system (IDS) & intrusion prevention system (IPS): Case study // International Journal of Scientific & Engineering Research. – 2012. – T. 2. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ddcb13f5dc671786b6fef5aa1fc4cc0285c4c79d

3. Snort – Network Instruction Detection. URL: https://www.snort.org/

4. Hoover C. Comparative study of snort 3 and suricata intrusion detection systems. – 2022. URL: https://scholarworks.uark.edu/csceuht/105/

5. Home – Suricata. URL: https://suricata.io/

6. Ford M. et al. The process of transferring Fail2ban data to an adaptive corporate intrusion detection and prevention system // SoutheastCon 2016. – IEEE, 2016. – pp. 1-4. URL: https://iocscience.org/ejournal/index.php/mantik/article/view/673/434

7. How to secure SSH using Fail2Ban. A beginner's guide. URL: https://itshaman.ru/articles/3016/kak-zashchitit-ssh-s-pomoshchyu-fail2ban-rukovodstvo-dlya-nachinayushchikh

8. Security of network connections. URL: https://maximalisimus.github.io/Articles/The-security-of-network-connections.html#part5.0

9. OSSEC – World`s Most Widely Used Host Intrusion Detected System – HIDS. URL: https://www.ossec.net/

10. Teixeira D. et al. OSSEC IDS extension to improve log analysis and override false positive or negative detections //Journal of Sensor and Actuator Networks. – 2019. – T. 8. – №. 3. – C. 46. URL: https://www.mdpi.com/2224-2708/8/3/46.

11. Pilkevich P.V., Maslova M.A. The influence of relational database indexes on search performance // Threats and risks in the South of Russia in the context of the geopolitical crisis. Achievements and prospects for scientific research of young scientists in the South of Russia: Materials of scientific events: All-Russian conference with international participation; XIX Annual Youth Scientific Conference, Rostov-on-Don, March 15 – 29, 2023. – Rostov-on-Don: Federal State Budgetary Institution of Science "Federal Research Center Southern Scientific Center of the Russian Academy of Sciences", 2023. – P. 310.

12. Implementation of ESG principles in the development strategy of the Russian economy / N.G. Vovchenko, N.G. Kuznetsov, E.N. Makarenko [etc.]. – Rostov-on-Don: Rostov State Economic University “RINH”, 2022. – 508 p.

Надейкина Виктория Сергеевна, студент четвертого курса кафедры «Информационная безопасность»
Маслова Мария Александровна, доцент кафедры «Информационная безопасность»

Nadeykina Victoria Sergeevna, fourth year student of the Department of Information Security
Maslova Maria Aleksandrovna, Associate Professor of the Department of Information Security