БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 3 (110). – 54–66

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-3-54-66

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Е.Ю. СОЛДАТОВ[1], В.В. СЕЛИФАНОВ[2], М.А. КУВШИНОВ[3]

[1] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, лаборант. E-mail: wilgieforz@mail.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель. E-mail: sfo1@mail.ru,* ORCID ID: 0000-0002-6691-5647

[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: kuvshinovma@gmail.com*

Целью настоящей работы является разработка системы контроля инцидентов информационной безопасности, отвечающей требованиям к регистрируемой информации и инцидентам информационной безопасности. В статье поднимается вопрос необходимости создания системы, которая позволит контролировать инциденты информационной безопасности, проводить оценку существующих решений на рынке, формировать требования для системы, выбор и обоснование технологий при разработке. После регистрации инцидента есть возможность взаимодействия с другими узлами сети, блокировки IP-адреса источника на МЭ веб-сервера (iptables), закрытия сетевого порта, блокировки доменов на прокси-сервере. Также реализован функционал просмотра данной информации в веб-интерфейс системы. В статье описана и обоснована необходимость создания и внедрения такой системы в информационную сеть. Для достижения поставленной цели был проведен анализ рынка аналогичных систем, а также проблем при их сопровождении. Исходя из анализа было разработано техническое задание с последующей реализацией программного кода, проведена апробация системы и реализовано несколько сценариев. В работе был проведен анализ методических документов, связанных с инцидентами информационной безопасности, разработано техническое задание, реализован программный код, проведена апробация. В результате было разработано программное обеспечение «Система контроля инцидентов информационной безопасности».

Ключевые слова: информационная безопасность, инцидент информационной безопасности, расследование, кибербезопасность, система обнаружения вторжений, система предотвращения вторжений, межсетевой экран, прокси-сервер

* Статья получена 03 июля 2023 г.

ВВЕДЕНИЕ

В связи с тем, что атаки на информационные системы организаций с каждым годом становятся всё чаще, масштабнее и серьезнее, возрастают масштабы негативных последствий, возникает потребность своевременно реагировать и регистрировать инциденты информационной безопасности, направленные на информационную систему. Для реализации этой задачи используется специальное программное обеспечение – система контроля инцидентов информационной безопасности IMS (Incident Management Software). На рынке представлено множество популярных решений для реализации данной задачи, но практически все из них – реализации иностранных государств.

Президентом Российской Федерации в 2022 году было утверждено два указа:

– Указ Президента РФ от 30.03.2022 № 166 о том, что с 31 марта 2022 года были введены ограничения на приобретение иностранного оборудования и программного обеспечения для субъектов КИИ, а также услуги по использованию такого ПО без согласования с уполномоченным органом [1];

– Указ Президента РФ от 01.05.2022 № 250 о том, что с 1 января 2025 года организациям запрещается использовать средства защиты информации, произведенные в недружественных государствах [2].

Также с 13 февраля 2023 года вступил в силу приказ ФСБ России № 77, утверждающий порядок взаимодействия операторов с ГосСОПКА на информационных ресурсах РФ, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных [3].

Таким образом, можно утверждать, что обеспечение отечественной системой контроля инцидентов информационной безопасности в защищаемую информационную систему – задача, актуальная для каждой организации.

Целью настоящей работы является создание системы контроля инцидентов информационной безопасности, которая должна решить проблемы, упомянутые выше, и будет проста во внедрении и сопровождении.

Для достижения данной цели были поставлены следующие задачи:

1) разработка требований к создаваемой системе;

2) разработка системы контроля инцидентов информационной безопасности;

3) внедрение системы и ее апробация.

1. РАЗРАБОТКА ТРЕБОВАНИЙ К СИСТЕМЕ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление инцидентами кибербезопасности не является линейным процессом. Это цикл, состоящий из подготовки, обнаружения, сдерживания, ликвидации и восстановления. Заключительный этап состоит из извлечения уроков из инцидента с целью улучшения процесса и подготовки к будущим возможным сценариям. После каждого инцидента следует организовать обзорное собрание с участием команды специалистов отдела ИБ, руководства организации и каждого отдельного сотрудника, чтобы сделать соответствующие выводы и проанализировать эффективность плана реагирования на инциденты и стратегии на каждом его этапе. Жизненный цикл инцидента информационной безопасности представлен на рис. 1.

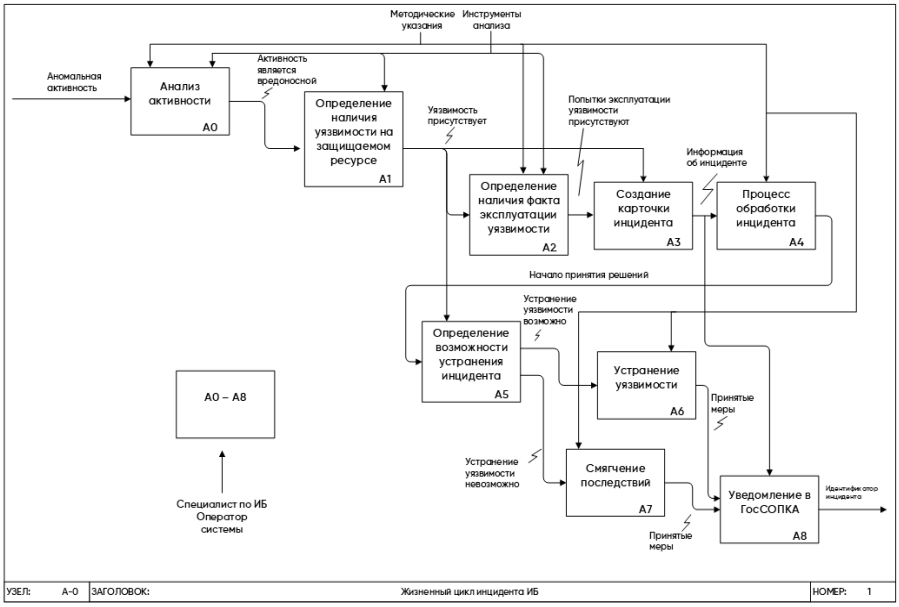

Рис. 1. Жизненный цикл инцидента ИБ

Fig. 1. Life cycle of an information security incident

Современные системы контроля инцидентов информационной безопасности, как ни странно, выполняют функции регистрации инцидентов ИБ и

позволяют удобно отслеживать, в каком состоянии они находятся. Инцидент после отработки сохраняется в базе данных для возможного дальнейшего извлечения уроков из него.

Современный рынок характеризуется сравнительно небольшим выбором систем – как коммерческих, так и с открытым исходным кодом. Первые отличаются высокой стоимостью, оправданной наличием сертификатов соответствия техническим требованиям, предъявляемым регуляторами в сфере информационной безопасности: если в сети обрабатывается информация, подлежащая обязательной защите в соответствии с действующим законодательством, то допускается использование только сертифицированных средств защиты, прошедших процедуру оценки ФСБ России и ФСТЭК России. Второй тип решений, состоящих из приложений с открытым исходным кодом, не менее распространен ввиду своей доступности. Такие системы зачастую используются в средствах защиты информации, к которым не предъявляются строгие требования регуляторов (в частности, в отношении сертификации средств защиты информации), или служат основой для создания коммерческих решений, разрабатываемых частными компаниями. Главной проблемой рассматриваемых систем с открытым исходным кодом является то, что они не специализируются на инцидентах информационной безопасности: практически все из них – реализация для Service Desk (техническая поддержка).

Ввиду невозможности использования дорогостоящих коммерческих систем с целью разбора функционала для реализации задач данной работы далее будут рассмотрены некоторые популярные коммерческие решения из обзорных статей на сайтах производителей.

Security Vision Incident Response Platform (IRP / SOAR) – российское программное обеспечение для автоматизации действий по реагированию на инциденты кибербезопасности. Этот программный продукт позволяет автоматически выполнять дежурные назначения в режиме реального времени. Модуль IRP позволяет автоматически реагировать на инциденты кибербезопасности (попытки внедрения ВПО, попытки эксплуатации уязвимостей, активность ВПО в сети, нарушение политик и др.), благодаря чему снижается риск человеческого фактора и ошибок операторов, ответственных за реагирование на инциденты информационной безопасности [4].

Security Vision Security Operation Center (SOC) – российский программный продукт, предназначенный для создания собственного глобального центра мониторинга информационной безопасности в масштабах организации, города, страны или мира. Это программное обеспечение обладает полным функционалом для построения и визуализации процессов информационной без-

опасности в режиме реального времени на масштабируемой карте. Благодаря этому операторы SOC получают полную информацию и аналитику в режиме online, а значит, могут оперативно реагировать на инциденты любой сложности. В данном программном продукте есть функция обмена информацией об инцидентах с государственными и коммерческими центрами мониторинга, такими как ГосСОПКА, ФинЦЕРТ и другие [5].

R-Vision SOAR (ранее R-Vision IRP) – это программный продукт для автоматизации деятельности по мониторингу, регистрации и реагированию на инциденты информационной безопасности. Позволяет получать данные об инцидентах с SIEM, СЗИ и других источников. Собственные правила и источники Threat Intelligence позволяют корректно среагировать на событие информационной безопасности, зарегистрировать инцидент и подробно его описать.

Благодаря функционалу R-Vision SOAR специалисты центра мониторинга имеют возможность удобно взаимодействовать и обмениваться информацией с ГосСОПКА, ФинЦЕРТ и MSS-провайдерами об инцидентах в информационной сети [6].

TheHive – это масштабируемая IRP, тесно интегрированная с MISP (платформой для обмена информацией о вредоносных программах), предназначена для упрощения работы SOC, CSIRT, CERT и любых специалистов по информационной безопасности, имеющих дело с инцидентами кибербезопасности, которые необходимо расследовать и оперативно на них реагировать. Считается лидером среди программ с открытым исходным кодом.

TheHive позиционируется как продукт 4-in-1 и содержит в себе:

– ядро системы, в котором происходит основной рабочий процесс;

– интегрированная система поиска Cortex, благодаря которой осуществляется анализ событий и механизм активного реагирования;

– агрегатор каналов узлов Hippocampe, объединяющий индикаторы компрометации из множества открытых источников в кластере Elacticsearch;

– REST API клиент TheHive4Py для написания скриптов на Python под любые нужды.

Программный код TheHive реализован на языке Scala и на текущий момент поддерживает ELK 5/6 для хранения логов. Клиентская часть системы реализована на JavaScript с использованием платформы для разработки веб-приложений AngularJS в паре с набором инструментов Bootstrap [7].

Данная система проста как в установке, так и в использовании с теми возможностями «из коробки», которых достаточно для выполнения большинства базовых задач.

2. РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Что такое стек технологий для веб-разработки? Стек веб-разработки относится к комбинации инструментов и технологий, используемых для создания веб-приложения. Стеки технологий веб-разработки включают в себя все языки программирования, фреймворки, библиотеки, серверы, программное обеспечение, используемые веб-разработчиками для написания проекта. Хотя веб-разработчики могут свободно создавать стеки в соответствии со своими потребностями, некоторые технологические стеки настолько хорошо работают вместе, что стали стандартами в индустрии веб-разработки. Они отлично себя зарекомендовали, так как позволяют работать более эффективно, устранять лишние ошибки и ускорять процесс разработки.

Для реализации программного кода и архитектуры приложения за основу был взят стек технологий PERN (PostgreSQL, Express, React, Node.js) [8]. LAMP – программное обеспечение с открытым исходным кодом, которое обычно устанавливается на сервер для отображения динамических веб-сайтов и веб-приложений. Обозначает операционную систему Linux с установленным веб-сервером Apache, базой данных MySQL для хранения информации сайта и его пользователей и PHP для обработки динамического контента.

Ruby on Rails – фреймворк для построения веб приложений на языке Ruby, использующий реляционные и NoSQL БД (MySQL, MariaDB, PostgreSQL и MondoDB).

Для реализации полноценного веб-приложения технологический стек PERN подходит лучше всего, так как язык, на котором реализуется программный код – JavaScript. Также у данного стека отличная масштабируемость, низкие системные требования для серверного оборудования и высокая производительность благодаря асинхронному выполнению кода, что позволяет обрабатывать запросы от тысячи пользователей.

Само веб-приложение будет построено на клиент-серверной архитектуре (рис. 2). Это означает, что приложение разделено на два звена – клиент и сервер. Клиент и сервер можно считать отдельным программным обеспечением. Поскольку серверная часть приложения должна выполнять множество запросов от различных клиентов, то ее необходимо размещать на выделенном сервере с высокой производительностью и пропускной способностью.

В качестве операционной системы на серверной части веб-приложения будет использоваться отечественная операционная система специального назначения Astra Linux Special Edition (Релиз «Смоленск») [9], в качестве БД выступает PostgreSQL.

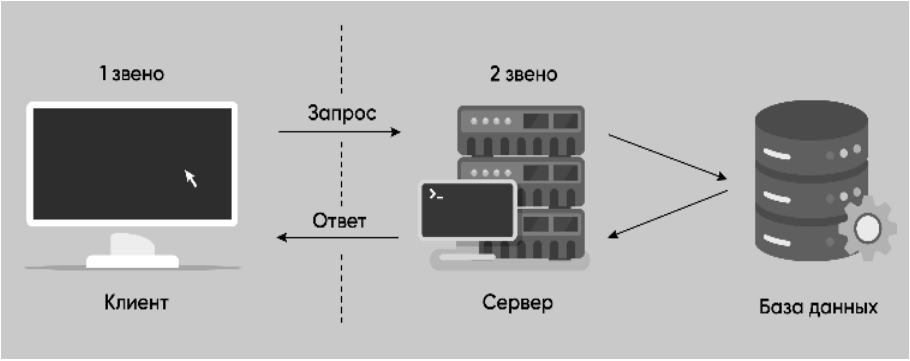

Рис. 2. Клиент-серверная архитектура

Fig. 2. Client-server architecture

Для реализации программного кода и архитектуры приложения за основу был взят стек технологий PERN (PostgreSQL, Express, React, Node.js) (рис. 3).

Рис. 3. Стек технологий PERN

Fig. 3. PERN technology stack

В результате дашборд и карточка инцидента выглядят следующим образом (рис. 4 и 5).

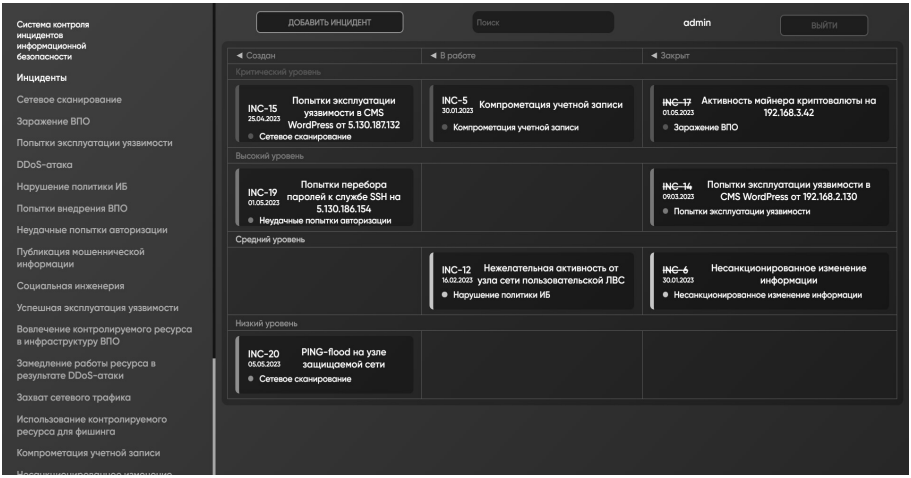

Рис. 4. Графическая панель с инцидентами

Fig. 4. Dashboard with incidents

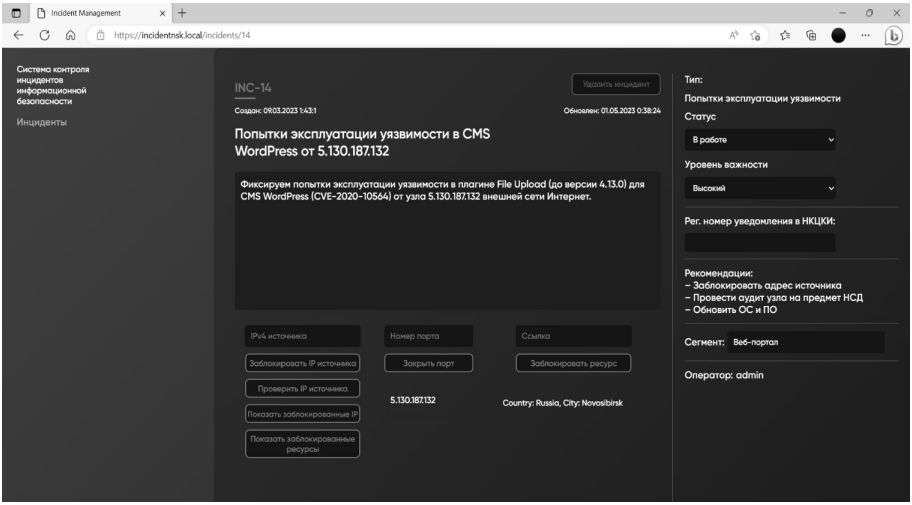

Рис. 5. Карточка инцидента ИБ

Fig. 5. Information security incident card

3. ВНЕДРЕНИЕ В КОМПЬЮТЕРНУЮ СЕТЬ

Информационная система была внедрена в компьютерную сеть с такими СЗИ, как ViPNet IDS NS, xFirewall и PT AF. Также вместе с ней был внедрен кэширующий проксисервер Squid для реализации функции блокировки URI сегмента Office Users (рис. 6).

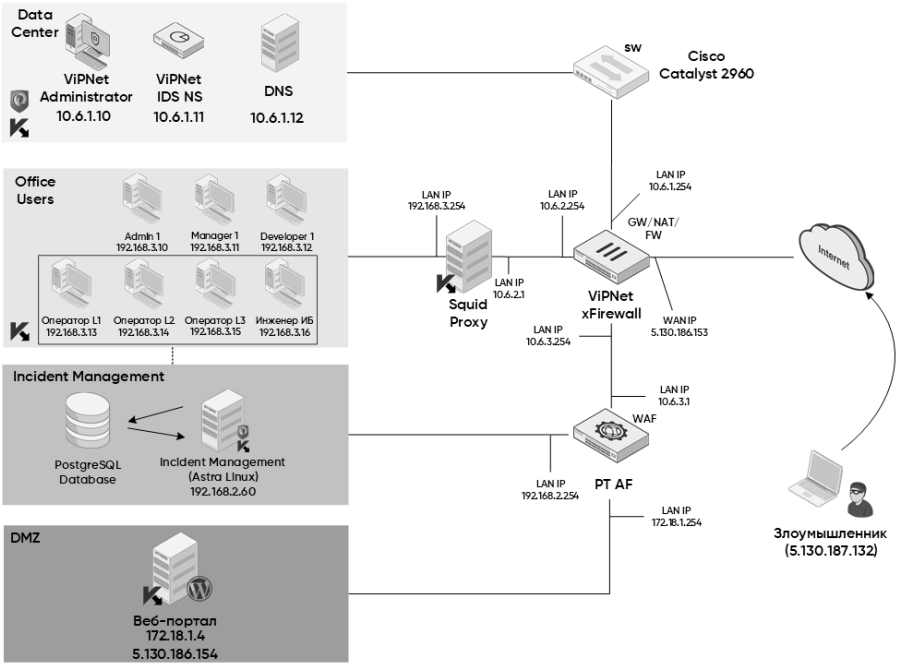

Рис. 6. Логическая схема компьютерной сети

Fig. 6. Logic diagram of a computer network

ЗАКЛЮЧЕНИЕ

Разработанная система контроля инцидентов информационной безопасности решает упомянутые ранее проблемы и позволяет эффективно регистрировать инциденты, собирает информацию в одном месте, передает его в ГосСОПКА (НКЦКИ) [10] с помощью электронной почты, а также имеет модуль управления инцидентом, позволяющий блокировать нежелательные IP, ресур-

сы и закрывать сетевые порты на встроенном межсетевом экране дистрибутива Linux iptables.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2022. – № 14. – Ст. 2242.

2. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2022. – № 18. – Ст. 3058.

3. Приказ ФСБ РФ от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с ГосСОПКА на информационные ресурсы, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (представление, распространение, доступ) персональных данных» // Официальный интернет-портал правовой информации (ФСБ России). – Опубл. 20.02.2023. – № 14.

4. Security Vision IRP: сайт. – URL: https://www.securityvision.ru/products/irp/ (дата обращения: 04.09.2023).

5. Security Vision SOC: сайт. – URL: https://www.securityvision.ru/products/soc/ (дата обращения: 04.09.2023).

6. R-Vision SOAR: сайт. – URL: https://rvision.ru/products/soar (дата обращения: 04.09.2023).

7. TheHive Project: сайт. – URL: https://thehive-project.org/ (дата обращения: 04.09.2023).

8. *Сафин А.М., Кадыров К.А.* Стек разработки приложений PERN // Актуальные вопросы общества, науки и образования: сборник статей Международной научно-практической конференции. – Пенза, 2022. – С. 95–97.

9. Astra Linux: сайт. – URL: https://astralinux.ru/ (дата обращения: 04.09.2023).

10. Приказ ФСБ РФ от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации (ФСБ России). – Опубл. 17.07.2019. – № 49.

Солдатов Егор Юрьевич, лаборант кафедры защиты информации Сибирского государственного университета геосистем и технологий. В настоящее время специализируется в области информационной безопасности. E-mail: wilgieforz@mail.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. В настоящее время специализируется в области информационной безопасности. E-mail: sfo1@mail.ru

Кувшинов Максим Алексеевич, ассистент кафедры защиты информации Новосибирского государственного технического университета. В настоящее время специализируется в области информационной безопасности. E-mail: kuvshinovma@gmail.com

DOI: 10.17212/2782-2230-2023-3-54-66

Development of the information security incident control system*

E.Yu. Soldatov[1], V.V. Selifanov[2], M.A. Kuvshinov[3]

[1] *Siberian State University of Geosystems and Technologies, 10 K. Plakhotnogo, Novosibirsk, 630108, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: wilgieforz@mail.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, assistant of the Department of Information Security. E-mail: kuvshinovma@gmail.com*

The purpose of this work is to develop an information security incident control system that meets the requirements for recorded information and information security incidents. the article raises the question of the need to create a system that will allow you to control information security incidents. Evaluation of existing solutions on the market, formation of requirements for the system. Selection and justification of technologies during development. After registering an incident, it is possible to interact with other network nodes, block the source IP address on the ME web server (iptables), close the network port, block domains on the proxy server. The functionality of viewing this information in the system web interface is also implemented. The article describes and substantiates the need to create and implement such a system in the information network. To achieve this goal, an analysis of the market for similar systems, as well as problems in their maintenance, was carried out. Based on the analysis, a technical task was developed with the subsequent implementation of the program code. The system was then tested and several work scenarios were implemented. In the work, an analysis of methodologi-

* *Received 03 July 2023.*

cal documents related to information security incidents was made, a technical task was developed, a program code was implemented, and testing was carried out. As a result, the software "Information Security Incident Control System" was developed.

Keywords: information security, information security incident, investigation, cybersecurity, intrusion detection system, intrusion prevention system, firewall, proxy server

REFERENCES

1. Ukaz Prezidenta RF ot 30.03.2022 № 166 «O merakh po obespecheniyu tekhnologi-cheskoi nezavisimosti i bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» [Decree of the President of the Russian Federation of March 30, 2022 No. 166 "On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation"]. *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation*, 2022, no. 14, art. 2242.

2. Ukaz Prezidenta RF ot 01.05.2022 № 250 «O dopolnitel'nykh merakh po obespecheniyu informatsionnoi bezopasnosti Rossiiskoi Federatsii» [Decree of the President of the Russian Federation of 01.05.2022 Nn. 250 "On additional measures to ensure information security of the Russian Federation"]. *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation*, 2022, no. 18, art. 3058.

3. [Order of the Federal Security Service of the Russian Federation dated February 13, 2023 No. 77 "On approval of the procedure for the interaction of operators with NCCCI on information resources, including informing the FSB of Russia about computer incidents that resulted in the unlawful transfer (presentation, distribution, access) of personal data"]. *Ofitsial'nyi internet-portal pravovoi informatsii (FSB Rossii)* [Official Internet portal of legal information (FSB of Russia)], 2023, no. 14. (In Russian).

4. *Security Vision IRP*. Website. (In Russian). Available at: https://www.securityvision.ru/products/irp/ (accessed 04.09.2023).

5. *Security Vision SOC*. Website. (In Russian). Available at: https://www.securityvision.ru/products/soc/ (accessed 04.09.2023).

6. *R-Vision SOAR*. Website. (In Russian). Available at: https://rvision.ru/products/soar (accessed 04.09.2023).

7. *TheHive Project*. Website. Available at: https://thehive-project.org/ (accessed 04.09.2023).

8. Safin A.M., Kadyrov K.A. [PERN application development stack]. *Aktual'nye voprosy obshchestva, nauki i obrazovaniya* [Actual issues of society, science and education]. Collection of materials of the International scientific and practical conference, Penza, 2022, pp. 95–97. (In Russian).

9. *Astra Linux*. Website. (In Russian). Available at: https://astralinux.ru/ (accessed 09.04.2023).

10. [Order of the Federal Security Service of the Russian Federation of June 19, 2019 No. 282 "On approval of the Procedure for informing the FSB of Russia about computer incidents, responding to them, taking measures to eliminate the consequences of computer attacks carried out in relation to significant objects of the critical information infrastructure of the Russian Federation"]. *Ofitsial'nyi internet-portal pravovoi informatsii (FSB Rossii)* [Official Internet portal of legal information (FSB of Russia)], 2019, no. 49. (In Russian).

Для цитирования:

Солдатов Е.Ю., Селифанов В.В., Кувшинов М.А. Разработка системы контроля инцидентов информационной безопасности // Безопасность цифровых технологий. – 2023. – № 3 (110). – С. 54–66. – DOI: 10.17212/2782-2230-2023-3-54-66.

For citation:

Soldatov E.Yu., Selifanov V.V., Kuvshinov M.A. Razrabotka sistemy kontrolya intsidentov informatsionnoi bezopasnosti [Development of the information security incident control system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 3 (110), pp. 54–66. DOI: 10.17212/2782-2230-2023-3-54-66.