http://dx.doi.org/10.35596/1729-7648-2026-24-1-60-67

УДК 004.056

АНАЛИЗ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В. А. ГЕРАСИМОВ[1,2], О. В. БОЙПРАВ[2], Р. Н. РУСЕЦКИЙ[2]

[1]Научно-исследовательский институт технической защиты информации (Минск, Республика Беларусь)
[2]Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. В статье анализируются события информационной безопасности в системе электронной цифровой подписи на основе виртуальной инфраструктуры согласно требованиям положения о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности. Рассмотрены ключевые модули системы: модуль аутентификации, модуль выработки электронной цифровой подписи и модуль ее проверки, включая их подмодули для защиты данных, формирования подписей и верификации. Приведены примеры событий для журналирования, такие как аутентификация пользователей, формирование электронных документов, передача хэш-значений, признаки киберинцидентов, включая аномальные действия пользователей. Представлены события информационной безопасности, журналируемые в системах электронной цифровой подписи на основе виртуальной инфраструктуры. Выполнена оценка соответствия результатов журналирования этих событий требованиям, представленным в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130.

Ключевые слова: событие информационной безопасности, электронная цифровая подпись, сравнительный анализ, виртуальная инфраструктура.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Герасимов, В. А. Анализ событий информационной безопасности в системе электронной цифровой подписи на основе виртуальной инфраструктуры / В. А. Герасимов, О. В. Бойправ, Р. Н. Русецкий // Доклады БГУИР. 2026. Т. 24, № 1. С. 60–67. http://dx.doi.org/10.35596/1729-7648-2026-24-1-60-67.

ANALYSIS OF INFORMATION SECURITY EVENTS IN AN ELECTRONIC DIGITAL SIGNATURE SYSTEM BASED ON A VIRTUAL INFRASTRUCTURE

VIACHESLAU GERASIMOV[1,2], OLGA BOIPRAV[2], ROMAN RUSETSKI[2]

[1]Research Institute for Technical Protection of Information (Minsk, Republic of Belarus)
[2]Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. This article analyzes information security events in a virtual infrastructure-based electronic digital signature system in accordance with the requirements of the regulations on the procedure for information exchange between elements of the national cybersecurity system. Key system modules are considered: the authentication module, the electronic digital signature generation module, and the verification module, including their submodules for data protection, signature generation, and verification. Examples of events for logging are provided, such as user authentication, electronic document generation, hash value transfer, and indicators of cyber incidents, including abnormal user actions. Information security events logged in virtual infrastructure-based electronic digital signature systems are presented. An assessment is made of the compliance of the logging results for these events with the requirements set out in Order No 130 of the Operational and Analytical Center under the President of the Republic of Belarus dated July 25, 2023.

Keywords: information security event, electronic digital signature, comparative analysis, virtual infrastructure.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Gerasimov V., Boiprav O., Rusetski R. (2026) Analysis of Information Security Events in an Electronic Digital Signature System Based on a Virtual Infrastructure. *Doklady BGUIR*. 24 (1), 60–67. http://dx.doi.org/10.35596/1729-7648-2026-24-1-60-67 (in Russian).

Введение

С момента введения в жизнь человечества информационно-коммуникационных технологий (ИКТ) они стали фундаментом современного государственного управления, бизнеса и мировой экономики. Страны мира активно используют преимущества ИКТ, однако их повсеместное распространение привело к экспоненциальному росту объема информации, которая сегодня сравнивается с «новой нефтью». Этот прогресс сопровождается новыми рисками, вызовами и угрозами, поскольку зависимость общества от ИКТ растет, а сами технологии остаются изначально уязвимыми. Конфиденциальность, целостность и доступность информации постоянно подвергаются угрозам от быстро эволюционирующих рисков киберпространства. В критической точке находится доверие населения и организаций к ИКТ, которое подрывается отсутствием адекватной кибербезопасности[1].

Одним из ключевых элементов современной информационной инфраструктуры является технология электронной цифровой подписи (ЭЦП), особенно в форме системы ЭЦП на основе виртуальной инфраструктуры (ЭЦПВИ). Событие информационной безопасности в контексте системы ЭЦПВИ – это идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности, отказ средств защиты информации или ранее неизвестную ситуацию, связанную с угрозой [1]. Классификация событий информационной безопасности в системе ЭЦПВИ на основе виртуальной инфраструктуры становится неотъемлемой частью стратегии кибербезопасности. Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности[2]. Это более широкое понятие, включающее не только события, но и инциденты, такие как успешные атаки, утечки данных или сбои в работе. Классификация позволяет систематизировать угрозы по типам (например, по степени воздействия, по источнику атаки или уязвимостям инфраструктуры), что облегчает разработку мер реагирования и профилактики [2].

В условиях виртуальной среды, где ресурсы распределены и динамичны, классификация помогает выделить инциденты, связанные с облачными сервисами, виртуализацией или сетевыми протоколами. Это способствует скоординированным действиям государственных органов и организаций, как предусмотрено рекомендациями Национального центра кибербезопасности Оперативно-аналитического центра при Президенте Республики Беларусь. В контексте национальной безопасности Беларуси классификация событий информационной безопасности системы ЭЦПВИ напрямую способствует обеспечению безопасного функционирования объектов информационной инфраструктуры. Классификация не только помогает минимизировать последствия кибератак, но и укрепляет доверие к ИКТ как катализаторам экономического роста и социального развития. Введение такой классификации требует интеграции мониторинга, анализа и реагирования в повседневную практику, что позволит своевременно адаптироваться к новым угрозам.

Цель представленных в статье исследований – анализ событий информационной безопасности в системе ЭЦПВИ с учетом требований, изложенных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130. Для достижения цели решались следующие задачи:

[1] Рекомендации государственным органам и иным организациям (в том числе владельцам критически важных объектов информатизации) по выполнению обязательных для исполнения требований законодательства в сфере обеспечения кибербезопасности, в том числе технической и криптографической защиты информации [Электронный ресурс]. Режим доступа: https://www.oac.gov.by/public/content/files/files/recom.pdf. Дата доступа: 29.11.2025.

[2] О кибербезопасности: Указ Президента Республики Беларусь от 14 февраля 2024 г. № 40 [Электронный ресурс]. Режим доступа: https://www.oac.gov.by/public/content/files/files/law/decrees-rb/2023-40.pdf. Дата доступа: 29.11.2025.

– определение событий в системе ЭЦПВИ, подлежащих журналированию, с выявлением киберинцидентов в такой системе;

– оценка соответствия результатов журналирования этих событий требованиям, представленным в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130.

Анализ событий системы электронной цифровой подписи на основе виртуальной инфраструктуры

Система ЭЦПВИ представляет собой программно-аппаратный комплекс для выработки ЭЦП и формирования электронного документа (ЭД). Систему можно разделить на несколько модулей.

• Модуль аутентификации. Предназначен для аутентификации сторон, где одной стороной является клиент системы, который с помощью клиентской программы и прикладной системы аутентифицируется в системе ЭЦПВИ, а второй – сама система ЭЦПВИ. Модуль разделен на подмодули, один из которых обеспечивает защиту канала передачи данных с помощью средства линейного шифрования согласно п. 17 перечня государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность» приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 28 декабря 2022 г. № 207 для обеспечения конфиденциальности передаваемых данных. Другой подмодуль, частично соответствующий СТБ 34.101.87–2022 «Информационные технологии и безопасность. Инфраструктуры аутентификации», обеспечивает аутентификацию пользователя[3]. При этом, если система ЭЦПВИ используется внутри криптографической границы, подмодуль линейного шифрования может быть отключен, а защита передаваемых данных может обеспечиваться с помощью штатных средств, применяемых внутри защищенного периметра.

• Модуль выработки ЭЦП. Предназначен для выработки значения ЭЦП и формирования ЭД. Разделен на подмодули, один из которых обеспечивает формирование подписанных данных с использованием алгоритмов хэширования согласно п. 5 перечня государственных стандартов, взаимосвязанных с ТР 2013/027/BY для обеспечения целостности данных перед подписанием. Другой подмодуль, соответствующий СТБ 34.101.45–2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых», обеспечивает выработку ЭЦП на основе асимметричных криптографических алгоритмов. Третий подмодуль обеспечивает технологическую проверку значения ЭЦП перед формированием ЭД.

• Модуль проверки ЭЦП. Обеспечивает проверку ЭЦП ЭД на основе асимметричных криптографических алгоритмов, соответствует СТБ 34.101.45–2013.

Событиями, которые подлежат журналированию в каждом модуле системы ЭЦПВИ, являются [1]:

– использование личного ключа пользователя;

– аутентификация пользователей в системе;

– получение электронного документа или его хэш-значения;

– начало и окончание формирования документа пользователем;

– получение от пользователя подтверждения на подпись документа;

– передача хэш-значения подписанных данных пользователя между компонентами системы;

– получение значения ЭЦП;

– выгрузка и отправка ЭД пользователю.

Киберинцидентами в системе ЭЦПВИ являются:

– действия пользователя в ночное время;

– действия пользователя, выполняемые с аномальной скоростью;

[3] Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов, М. А. Казловский, О. В. Бойправ // Комплексная защита информации: матер. XXVIII науч.-практ. конф., г. Гомель, 23–25 мая 2023 г. Гомель: Белор. гос. ун-т трансп., 2023. С. 257–261. https://libeldoc.bsuir.by/handle/123456789/52449.

– действия пользователя, пропускающие стандартные действия в рамках определенных процессов;

– дублирование пользовательских сеансов.

Для организации процессов анализа, обнаружения и реагирования на киберинциденты [3] необходимо обеспечить централизованный сбор и обработку событий с использованием SIEM-системы. Способ сбора событий определяется исходя из функциональных возможностей системы ЭЦПВИ. SIEM-система обеспечивает как активный, так и пассивный сбор событий с источников данных. При пассивном сборе событий SIEM-система ожидает событий от удаленного сервера [4], что является более предпочтительным с точки зрения экономии вычислительных ресурсов и трудозатрат на настройку, при активном – инициирует подключение к источнику событий [5].

Средством для организации активного сбора событий выступает агент либо коннектор SIEM-системы. После организации получения событий в SIEM-систему реализуются такие этапы обработки, как парсинг, фильтрация, агрегация, обогащение и корреляция. Для нормализации входящих потоков данных используются базовые парсеры [6], работающие с распространенными форматами данных [7] (syslog, json, CEF). При необходимости может потребоваться дополнительная разработка регулярных выражений.

Система ЭЦПВИ протоколирует события в виде строки или JSON-объекта. Первый вариант удобен для прочтения человеком и ручного анализа киберинцидентов [8]. Вариант протоколирования событий в виде JSON-объекта подходит для передачи этих событий в SIEM-систему, так как написание парсера для JSON-объекта проще, чем для строки. Примерами протоколируемых событий в виде строки являются:

13.11.2025 14:56:16.442 [INFO] session_code = REQUEST STARTED from address: 10.233.105.222, [NameService] /api/vn/name”

13.11.2025 14:56:16.442 [INFO] session_code = empty, [NameService] start auth

13.11.2025 14:56:16.442 [INFO] session_code = 248d1303, [NameService] user with ID=5 auth success in system!

13.11.2025 14:56:16.442 [INFO] session_code = 248d1303, [NameService] user with ID=5 auth success in system!

13.11.2025 14:56:16.442 [WARNING] session_code = 248d1303, [NameService] user with ID=5 incorrect OTP!

13.11.2025 11:16:15.101 [ERROR] session_code = 248d1303, [NameService] user with ID=5 enter incorrect OTP 3 times!

13.11.2025 11:16:15.123 [INFO] session_code=248d1303, [NameService] finish auth

13.11.2025 14:36:23.433 [INFO] session_code = REQUEST FINISHED from address: 10.233.105.222, [NameService] /api/vn/name”

В виде JSON-объекта событие выглядит следующим образом:

{“message”: “REQUEST STARTED from address: 10.233.105.222, [NameService] /api/vn/name”, “service”: “NameService”, “session_code”: “REQUEST STARTED”, “timestamp”: “13.11.2025 14:56:16.442”, “type”: “INFO”}

{“message”: “start auth”, “service”: “NameService”, “session_code”: “empty”, “timestamp”: “13.11.2025 14:56:16.442”, “type”: “INFO”}

{“message”: “user with ID=5 auth success in system!”, “service”: “NameService”, “session_code”: “248d1303”, “timestamp”: “13.11.2025 14:56:16.442”, “type”: “INFO”}

{“message”: “user with ID=5 auth success in system!”, “service”: “NameService”, “session_code”: “248d1303”, “timestamp”: “13.11.2025 14:56:16.442”, “type”: “INFO”}

{“message”: “user with ID=5 incorrect OTP!”, “service”: “NameService”, “session_code”: “248d1303”, “timestamp”: “13.11.2025 14:56:16.442”, “type”: “WARNING”}

{“message”: “user with ID=5 enter incorrect OTP 3 times!”, “service”: “NameService”, “session_code”: “248d1303”, “timestamp”: “13.11.2025 11:16:15”, “type”: “ERROR”}

{“message”: “finish auth”, “service”: “NameService”, “session_code”: “248d1303”, “timestamp”: “13.11.2025 11:16:15.11”, “type”: “INFO”}

{“message”: “REQUEST FINISHED from address: 10.233.105.222, [NameService] /api/vn/name”, “service”: “NameService”, “session_code”: “REQUEST FINISHED”, “timestamp”: “13.11.2025 14:36:23.433”, “type”: “INFO”}

Под расширенными методами определения киберинцидентов будет пониматься метод, при котором происходят сбор и предобработка критических данных системы, а после на основе расчета статистических показателей и определения пороговых значений будет дан вердикт о том, что событие является киберинцидентом или же нет. Данный метод описан в [1]. По результатам работы метода система ЭЦПВИ также сгенерирует событие, описанное выше.

Результаты исследований и их обсуждение

С целью анализа событий, подлежащих журналированию [9, 10], были рассмотрены требования к информационным системам приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130. На основе требований построена табл. 1 по журналированию событий в системе ЭЦПВИ.

Таблица 1. Выполнение требований для прикладного программного обеспечения
Table 1. Fulfilment of requirements for application software

Требование	Требование выполняется	Обоснование
Аутентификация (вход и (или) выход) пользователей	Да	Журналируются сведения о событиях типа «аутентификация пользователей в системе» (сведения о неуспешных попытках аутентификации и выходе из системы)
Успешные и неуспешные попытки аутентификации	Да	Журналируются сведения о событиях типов «ввод данных аутентификации в системе», «доступ к личному ключу»
Создание, копирование, перемещение, удаление, модификация учетных записей пользователей и конфигурационных файлов	Частично	В системе ЭЦПВИ за создание, копирование, перемещение, удаление, модификацию учетных записей пользователей отвечает отдельный компонент, протоколирование работы с конфигурационным файлом осуществляется средствами операционной системы
Неудавшиеся или отмененные действия пользователей	Да	Журналируются сведения о событиях, связанных с неудавшимися или отмененными действиями пользователей (создание ЭД, закрытие сессии (не выполнив процесс до конца))
Действия пользователей (доступ к объекту (данным), изменения объекта (данных), удаление объекта (данных))	Да	Журналируются сведения о событиях, связанных с получением доступа к объекту (данным), изменением объекта (данных), удалением объекта (данных)

Как следует из табл. 1, практически все требования к протоколированию событий соблюдаются. Среди выполняемых частично – управление учетными записями пользователей и модификация конфигурационных файлов. Они осуществляются другими компонентами, не рассмотренными в данной статье.

Был проведен анализ состава записи события информационной безопасности прикладного программного обеспечения, включающей поля на основе выполнения требований к записи события в системе ЭЦПВИ (табл. 2).

Таблица 2. Выполнение требований к записи события
Table 2. Meeting the event recording requirements

Требование	Требование выполняется	Обоснование
Дата и время возникновения события	Да	Все записи логов начинаются с даты и времени события
Наименование источника события (сервис и (или) служба)	Да	В каждой записи присутствует наименование источника (сервиса или службы)
Наименование учетных записей пользователей	Частично	Наименование учетных записей пользователя можно получить по полю session_code
IP-адрес источника	Да	В записи при первичном вызове контроллера присутствует IP-адрес источника

Окончание табл. 2
Ending of Tab. 2

Требование	Требование выполняется	Обоснование
IP-адрес хоста (устройств)	Частично	В записях сервиса нет данных об IP-адресе хоста. Его можно получить из логов модуля линейного шифрования
Время начала операции	Да	При первичном вызове контроллера присутствует запись с временем начала операции
Время окончания операции	Да	При завершении действий в контроллере присутствует запись с временем окончания операции
Описание события информационной безопасности	Да	Каждая запись содержит описание события

На основании проведенного анализа установлено, что большая часть требований к составу записей информационной безопасности в системе ЭЦПВИ соблюдается. Такие поля, как «Наименование учетных записей пользователей» и «IP-адрес хоста (устройств)», не указаны в записи явно, однако при включении в записи возможно наличие необходимой информации.

Заключение

1. Проведен сравнительный анализ событий информационной безопасности в системе электронной цифровой подписи на основе виртуальной инфраструктуры с требованиями приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130. Определены события для журналирования, а также форматы протоколирования (строковое представление и JSON-объект). Установлено, что журналирование сведений о событиях информационной безопасности в системе электронной цифровой подписи на основе виртуальной инфраструктуры практически в полной мере соответствует указанным требованиям. В частности, в записях о событиях информационной безопасности такой системы присутствуют следующие поля: дата и время возникновения события; наименование источника события; IP-адрес источника; время начала операции; время окончания операции; описание события информационной безопасности.

2. Расхождение журналирования сведений о событиях информационной безопасности в системе электронной цифровой подписи на основе виртуальной инфраструктуры с требованиями указанного приказа обусловлено тем, что в записях об указанных событиях отсутствуют такие поля, как наименование учетных записей пользователей и IP-адрес хоста (устройств). Для устранения расхождения целесообразно реализовать следующие решения в системе электронной цифровой подписи на основе виртуальной инфраструктуры:

– внедрить механизм автоматического извлечения и записи наименований учетных записей пользователей в запись события информационной безопасности, используя существующее поле session_code, чтобы обеспечить полное соответствие требованиям;

– реализовать сбор событий информационной безопасности с модуля линейного шифрования для протоколирования IP-адреса хоста (устройства), дополняя записи, где это поле отсутствует;

– обновить схему журналирования и форматы протоколирования в соответствии с требованиями, добавив указанные поля в обязательные атрибуты записей событий.

Список литературы

1. Герасимов, В. А. Метод обнаружения событий информационной безопасности в системах облачной подписи / В. А. Герасимов, О. В. Бойправ // Цифровая трансформация. 2024. Т. 30, № 2. С. 77–84. https://doi.org/10.35596/1729-7648-2024-30-2-77-84.
2. Микрюков, А. А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий / А. А. Микрюков, А. В. Бабаш, В. А. Сизов // Открытое образование. 2019. Т. 23, № 1. С. 57–63. https://doi.org/10.21686/1818-4243-2019-23-1-57-63.
3. Бойправ, В. А. Методика и программное средство для проведения аудита систем управления информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. 2022. Т. 19, № 4. С. 42–52. https://doi.org/10.37661/1816-0301-2022-19-4-42-52.

4. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке / С. И. Смирнов [и др.] // Российский технологический журнал. 2024. Т. 12, № 3. С. 25–36. https://doi.org/10.32362/2500-316X-2024-12-3-25-36.
5. Михайлова, В. Д. Описание инцидента при тестировании информационной безопасности киберфизических систем / В. Д. Михайлова // Инженерный вестник Дона. 2025. № 6.
6. Konchitchki, Y. Event Study Methodologies in Information Systems Research / Y. Konchitchki, D. E. O'Leary // International Journal of Accounting Information Systems. 2011. Vol. 12, Iss. 2. P. 99–115.
7. González-Granadillo, G. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures / G. González-Granadillo, S. González-Zarzosa, R. Diaz // Sensors. 2021. Vol. 21, No 14. https://doi.org/10.3390/s21144759.
8. Macaneata, C. Overview of Security Information and Event Management Systems / C. Macaneata // Informatica Economica, Academy of Economic Studies. 2024. Vol. 28, Iss. 1. P. 15–24.
9. Sayankar, V. N. A Review on Information Systems Audit / V. N. Sayankar // Research Journal of Engineering and Technology. 2024. Vol. 4, Iss. 3.
10. Vandapuye, S. An Overview of Information Systems in Auditing: Insights from Bibliometric Research / S. Vandapuye, S. Jabraoui // Salud, Ciencia y Tecnología – Serie de Conferencias. 2024. Vol. 3. DOI: 10.56294/sctconf20241013.

Поступила 10.12.2025 Принята в печать 05.01.2026

References

1. Gerasimov V. A., Boyprav O. V. (2024) Method for Information Security Events Detection in a Cloud Signature Systems. *Digital Transformation*. 30 (2), 77–84. https://doi.org/10.35596/1729-7648-2024-30-2-77-84 (in Russian).
2. Mikryukov A. A., Babash A. V., Sizov V. A. (2019) Classification of Events in Information Security Systems Based on Neural Networks. *Open Education*. 23 (1), 57–63. https://doi.org/10.21686/1818-4243-2019-23-1-57-63 (in Russian).
3. Boiprav V. A., Utin L. L. (2022) Methodology and Software Development for Auditing Information Security Management Systems. *Informatics*. 19 (4), 42–52. https://doi.org/10.37661/1816-0301-2022-19-4-42-52 (in Russian).
4. Smirnov S. I., Eremeev M. A., Magomedov Sh. G., Izerkin D. A. (2024) Criteria and Indicators for Assessing the Quality of the Investigation of an Information Security Incident as Part of a Targeted Cyberattack. *Russian Technological Journal*. 12 (3), 25–36. https://doi.org/10.32362/2500-316X-2024-12-3-25-36 (in Russian).
5. Mikhailova V. D. (2025) Description of an Incident During Testing of Information Security of Cyber-Physical Systems. *Engineering Bulletin of the Don*. (6) (in Russian).
6. Konchitchki Y., O'Leary D. E. (2011) Event Study Methodologies in Information Systems Research. *International Journal of Accounting Information Systems*. 12 (2), 99–115.
7. González-Granadillo G., González-Zarzosa S., Diaz R. (2021) Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 21 (14). https://doi.org/10.3390/s21144759.
8. Macaneata C. (2024) Overview of Security Information and Event Management Systems. *Informatica Economica, Academy of Economic Studies*. 28 (1), 15–24.
9. Sayankar V. N. (2024) A Review on Information Systems Audit. *Research Journal of Engineering and Technology*. 4 (3).
10. Vandapuye S., Jabraoui S. (2024) An Overview of Information Systems in Auditing: Insights from Bibliometric Research. *Salud, Ciencia y Tecnología – Serie de Conferencias*. 3. DOI: 10.56294/sctconf20241013.

Received: 10 December 2025 Accepted: 5 January 2026

Вклад авторов

Герасимов В. А. провел исследование, выполнил анализ полученных результатов, связанных с событиями информационной безопасности.

Бойправ О. В. осуществила постановку задачи исследования.

Русецкий Р. Н. провел исследование в рамках сбора событий информационной безопасности SIEM-системой.

Authors' contribution

Gerasimov V. conducted a study and performed an analysis of the obtained results related to information security events.

Boiprav O. carried out the formulation of the research task.

Rusetski R. conducted a study as part of the collection of information security events by the SIEM system.

Сведения об авторах

Герасимов В. А., магистр, сотр. Научно-исследовательского института технической защиты информации, асп. каф. защиты информации, Белорусский государственный университет информатики и радиоэлектроники (БГУИР)

Бойправ О. В., канд. техн. наук, доц., зав. каф. защиты информации, БГУИР

Русецкий Р. Н., магистрант каф. защиты информации, БГУИР

Адрес для корреспонденции

220088, Республика Беларусь,
Минск, ул. Первомайская, 26, корп. 2
Научно-исследовательский институт
технической защиты информации
Тел.: +375 17 302-81-71
E-mail: vger@niitzi.by
Герасимов Вячеслав Александрович

Information about the authors

Gerasimov V., M. Sci., Researcher at the Research Institute for Technical Protection of Information, Postgraduate at the Department of Information Protection, Belarusian State University of Informatics and Radioelectronics (BSUIR)

Boiprav O., Cand. Sci. (Tech.), Associate Professor, Head of the Department of Information Security, BSUIR

Rusetski R., Master's Student at the Department of Information Security, BSUIR

Address for correspondence

220088, Republic of Belarus,
Minsk, Pervomayskaya St., 26, Bld. 2
Research Institute
for Technical Protection of Information
Tel.: +375 17 302-81-71
E-mail: vger@niitzi.by
Gerasimov Viacheslau