http://dx.doi.org/10.35596/1729-7648-2024-30-2-77-84

*Оригинальная статья*
*Original paper*

УДК 004.056:004.056.5

# МЕТОД ОБНАРУЖЕНИЯ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ОБЛАЧНОЙ ПОДПИСИ

В. А. ГЕРАСИМОВ[1], О. В. БОЙПРАВ[2]

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

*Поступила в редакцию 18.12.2023*



**Аннотация.** Обоснованы параметры и механизмы, которые могут быть заложены в основу метода обнаружения событий информационной безопасности в системах облачной подписи, где используется протокол активации подписи, и разработка такого метода. В качестве указанных параметров предложены: количество подписываемых электронных документов, количество неверных попыток аутентификации для доступа к личному ключу пользователя, скорость сравнения хэш-значения подписываемых документов, скорость отправки хэш-значения подписываемых данных в устройстве создания подписи. Рекомендуется в основу метода заложить механизмы математической статистики применительно к перечисленным параметрам. Представлены описание и результаты апробации разработанного метода, количество ложноположительных и ложноотрицательных результатов анализа событий информационной безопасности в системах облачной подписи. Полученные значения оказались меньше аналогичных показателей, характерных для результатов анализа, проведенного с использованием других существующих методов. Это является основным преимуществом предлагаемого метода по сравнению с его аналогами.

**Ключевые слова:** SIEM-система, протокол активации подписи, профиль подписанта, система облачной подписи, событие информационной безопасности.

**Конфликт интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Для цитирования.** 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. http://dx.doi.org/10.35596/1729-7648-2024-30-2-77-84.

# METHOD FOR INFORMATION SECURITY EVENTS DETECTION IN A CLOUD SIGNATURE SYSTEMS

VYACHESLAV A. GERASIMOV[1], OLGA V. BOYPRAV[2]

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

*Submitted 18.12.2023*

**Abstract.** The parameters and mechanisms that can be used as the basis for a method for detecting information security events in cloud signature systems, where the signature activation protocol is used, and the development of such a method are substantiated. The following parameters are proposed: the number of signed electronic documents, the number of incorrect authentication attempts to access the user's personal key, the rate of comparing

the hash value of the signed documents, and the rate of sending the hash value of the signed data in the signature creation device. It is recommended to base the method on the mechanisms of mathematical statistics in relation to the listed parameters. The description and results of testing the developed method, the number of false positive and false negative results of the analysis of information security events in cloud signature systems are presented. The obtained values turned out to be less than similar indicators typical for the results of analysis carried out using other existing methods. This is the main advantage of the proposed method compared to its analogues.

**Keywords:** SIEM system, signature activation protocol, signer profile, cloud signature system, information security event.

**Conflict of interests.** The authors declare no conflict of interests.

**For citation.** Gerasimov V. A., Boyprav O. V. (2024) Method for Information Security Events Detection in a Cloud Signature Systems. *Digital Transformation.* 30 (2), 77–84. http://dx.doi.org/10.35596/1729-7648-2024-30-2-77-84 (in Russian).

## Введение

Система облачной подписи (СОП) является инструментом для создания электронных документов, подписанных личным ключом пользователя с использованием облачных технологий. Данная система позволяет создавать, хранить и обмениваться электронными документами, созданными в этой системе. Однако, как и любая другая информационная система, СОП подвержена различным угрозам информационной безопасности.

Определение событий информационной безопасности – важная составляющая обеспечения безопасности СОП. Событие информационной безопасности[1] – это идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или на отказ средств защиты информации, либо ранее неизвестная ситуация, которая может быть связана с угрозой информационной безопасности. Этот процесс может включать в себя такие шаги, как наблюдение, анализ и реагирование на различные события, которые могут указывать на нарушение безопасности или попытки несанкционированного доступа к личным данным либо к личному ключу пользователя.

Своевременное обнаружение событий информационной безопасности и реагирование на них позволяют администраторам СОП выявлять потенциальные угрозы и принимать соответствующие меры по обеспечению безопасности таких систем. Эти меры могут включать в себя формирование уведомлений о нарушениях, блокировку доступа к уязвимым ресурсам.

Цель представленных в статье исследований – обоснование параметров и механизмов, которые могут быть заложены в основу метода обнаружения событий информационной безопасности в системах облачной подписи, где используется протокол активации подписи (ПАП), и разработка такого метода. Для достижения цели решались следующие задачи:

1) анализ функций компонентов СОП;

2) классификация событий в СОП, подлежащих журналированию, и событий информационной безопасности в СОП;

3) классификация событий, регистрируемых SIEM-системами;

4) обоснование параметров, которые целесообразно применять при формировании профиля подписанта;

5) определение порядка реализации разработанного метода;

6) апробация разработанного метода.

## Метод анализа событий информационной безопасности при использовании протокола активации подписи

Протокол активации подписи применяется для обеспечения безопасного использования личного ключа при выработке значения облачной электронной цифровой подписи [1], выполняемой удаленным устройством создания подписи (УСП) от имени подписанта. ПАП используется в СОП, которая состоит из:

– сервера подписи (СП) – отвечает за проверку и передачу данных для выработки значения электронной цифровой подписи в УСП;

[1] Политика информационной безопасности [Электронный ресурс]. Режим доступа: https://www.nlb.by/content/o-biblioteke/politika-informatsionnoy-bezopasnosti/. Дата доступа: 13.12.2023.

– сервера документов (СД) – отвечает за создание и проверку электронных документов;

– сервера регистрации (СР) – отвечает за процессы, связанные с работой регистраторов регистрационных центров;

– УСП – отвечает за хранение личных ключей пользователей, процесс выработки значения электронной цифровой подписи (ЭЦП);

– клиентской программы пользователя/регистратора (КПП/КПР) – отвечает за предоставление интерфейса для выбора личного ключа/работы со слотами пользователя;

– прикладной системы (ПС) – отвечает за предоставление веб-интерфейса пользователям, регистраторам для взаимодействия с СОП.

В СОП базовыми событиями, которые подлежат журналированию и связаны с использованием ПАП, являются следующие действия:

– 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 СОП;

– получение значения ЭЦП;

– выгрузка и отправка электронного документа пользователю.

Схема взаимодействия между компонентами СОП представлена на рис. 1.

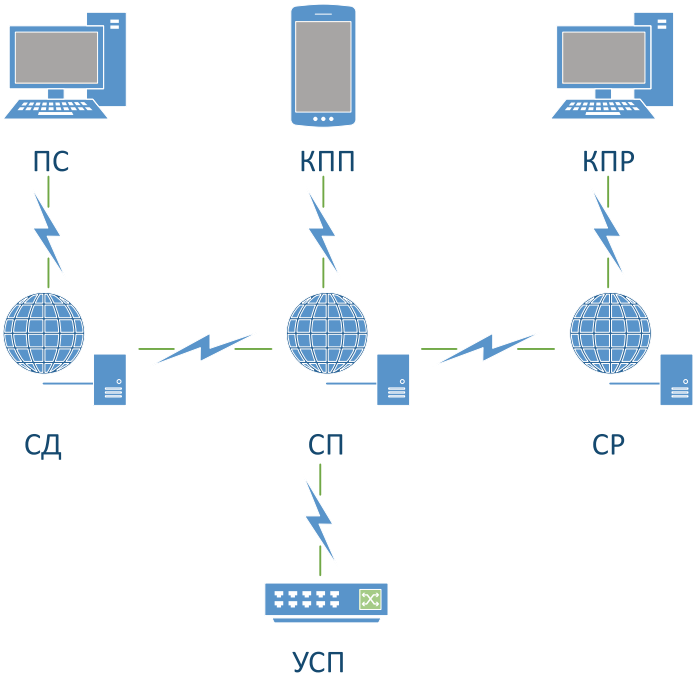


**Рис. 1.** Схема взаимодействия между компонентами системы облачной подписи
**Fig. 1.** Scheme of interaction between cloud signature system components

Событиями информационной безопасности в СОП, в которой используется ПАП, являются:

– действия пользователя в ночное время;

– действия пользователя, выполняемые с аномальной скоростью;

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

– дублирование пользовательских сеансов.

Для анализа событий информационной безопасности в информационных системах в настоящее время широко используются SIEM-системы, в основу алгоритмов работы которых заложены механизмы идентификации и классификации событий[2]. SIEM-системы регистрируют:

[2] SIEM-система [Электронный ресурс]. Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/?utm_referrer=https%3a%2f%2fwww.google.com%2f. Дата доступа: 13.12.2023.

1) события аутентификации и авторизации:
– успешная аутентификация пользователя;
– неудачная попытка аутентификации или ввод неправильного пароля;
– изменение привилегий или ролей пользователя;
2) события сетевой безопасности:
– обнаружение атаки на сетевой уровень, например, фильтрация пакетов или атака отказа в обслуживании (DoS);
– обнаружение вторжения или попытки взлома сетевых ресурсов;
– отказ в аутентификации на сетевом уровне;
3) События системной безопасности:
– обнаружение вредоносного программного обеспечения;
– обнаружение незаконных действий или нарушений политик безопасности;
– изменение конфигурации системы или нарушение целостности файловой системы;
4) события сбоев и угроз на уровне приложений:
– ошибки приложений или их некорректное поведение;
– попытки эксплойтов или использование известных уязвимостей в приложениях;
– изменение настроек или конфигурации приложений;
5) События управления угрозами:
– обнаружение подозрительной активности или аномалий в поведении пользователей или системы;
– обнаружение атаки на безопасность или нарушения политик безопасности;
– результаты анализа угроз и предупреждений о потенциальных угрозах.

Основной недостаток применяемых в настоящее время методов анализа событий информационной безопасности в информационных системах с помощью SIEM-систем состоит в том, что количество используемых в рамках указанных методов параметров, характеризующих контекст таких событий, недостаточно для того, чтобы установить характер поведения пользователя (злонамеренное или нет), которое обусловило их возникновение [2]. В связи с этим авторами предложено в основу метода анализа событий информационной безопасности в СОП, в которых используется ПАП, заложить выполнение анализа параметров цифрового образа пользователей этих систем, на основе которых можно установить, является ли выполнение протокола активации подписи обычным или же «аномальным». Под термином «цифровой образ»[3] следует понимать представление пользователя в информационной системе, являющееся виртуальным посредником между информационной системой и пользователем при доступе последнего к ресурсам этой системы. В системах, к которым пользователь обращается многократно, обычно гарантируется неизменность его цифрового образа при повторных обращениях. То есть цифровой образ пользователя является устойчивым, его принимают другие стороны и отождествляют с пользователем. Параметры цифрового образа включают в себя параметры профиля подписанта.

Предлагается заложить следующие четыре параметра профиля подписанта в основу метода анализа событий информационной безопасности в СОП, в которых используется ПАП:

1) количество подписываемых электронных документов;
2) количество неверных попыток аутентификации для доступа к личному ключу пользователя (максимальное значение – 3);
3) скорость сравнения хэш-значения подписываемых электронных документов;
4) скорость отправки хэш-значения подписываемых данных в УСП.

Выбор перечисленных параметров обусловлен тем, что они чаще всего являются идентификаторами нарушения цифрового образа. Для анализа перечисленных параметров предлагается использовать механизмы математической статистики. Разработанный метод, основанный на вышеуказанных параметрах и механизмах, включает в себя три этапа:

1) сбор и предобработку данных о количестве подписываемых документов, количестве неверных попыток аутентификации пользователя для доступа к личному ключу, скорость сравнения хэш-значений и скорость отправки хэш-значений в УСП;

2) расчет статистических показателей [3] для каждого параметра, а также определение пороговых значений. Вычисление статистических показателей, таких как среднее значение и стандартное отклонение, на основе полученных ранее данных. Среднее значение представляет сред-

[3] Информационные технологии и безопасность. Инфраструктуры аутентификации: СТБ 34.101.87–2022 [Электронный ресурс]. Режим доступа: https://apmi.bsu.by/assets/files/std/bias-spec130.pdf. Дата доступа: 13.12.2023.

нюю базовую точку для сравнения текущего события, а стандартное отклонение дает представление о разбросе данных. Пороговые значения рассчитываются путем добавления стандартных отклонений к среднему значению;

3) определение событий информационной безопасности, которое состоит:

– в анализе нового события путем сравнения значений текущих параметров с рассчитанными статистическими показателями;

– в классификации текущего события на основе сравнения текущих значений параметров с пороговыми значениями.

Если значения параметров выходят за пределы установленных пороговых значений, то событие может считаться событием информационной безопасности. В противном случае, если значения находятся в пределах пороговых значений, событие может быть классифицировано как нормальное.

**Результаты исследований и их обсуждение**

Для апробации разработанного метода была собрана фокус-группа, состоящая из 10 человек разного возраста (от 20 до 60 лет), с различным уровнем образования (среднее специальное, высшее). Участникам фокус-группы предоставили возможность изучить функционал СОП, после чего выполнить подписание ряда электронных документов с помощью ПС и КП, серверных компонентов СОП и УСП (количество документов – от одного до 10; количество итераций по подписанию каждого из документов – 20). Полученные по результатам каждой из итераций по подписанию электронного документа данные, представляющие собой значения приведенных выше параметров профиля каждого из подписантов из числа участников фокус-группы, группировались и записывались в базу данных (БД). В табл. 1 в качестве примера представлены полученные в ходе двадцати итераций по подписанию электронного документа данные профиля подписанта одного участника фокус-группы.

**Таблица 1.** Фрагмент данных, полученных от участника фокус-группы
**Table 1.** Fragment of data received from a focus group participant

| Номер итерации / Iteration number | Количество / Quantity | | Продолжительность / Duration | |
|---|---|---|---|---|
| | подписываемых документов / signed documents | неверных попыток аутентификации / invalid authentication attempts | сравнения хэш-значения, с / hash value comparisons, s | отправки хэш-значения, мс / sending hash value, ms |
| 1 | 9 | 1 | 1,24,49,23,38,6,46,45,3 | 41,56,57,53,58,4,22,12,42 |
| 2 | 1 | 0 | 51 | 32 |
| 3 | 3 | 1 | 8,19,23 | 21,6,46 |
| 4 | 4 | 0 | 45,12,34,39 | 3,32,1,49 |
| 5 | 1 | 0 | 52 | 45 |
| 6 | 5 | 1 | 32,55,3,26,34 | 42,30,30,26,6 |
| 7 | 4 | 1 | 42,42,40,16 | 20,24,23,4 |
| 8 | 2 | 1 | 1,37 | 18,26 |
| 9 | 2 | 0 | 57,25 | 20,18 |
| 10 | 4 | 0 | 28,53,33,5 | 36,37,46,45 |
| 11 | 8 | 1 | 43,20,1,11,36,39,52,2 | 36,27,43,5,10,32,26,49 |
| 12 | 8 | 1 | 10,4,49,23,1,14,6,56 | 42,47,38,28,53,2,37,23 |
| 13 | 7 | 0 | 45,56,1,38,50,52,25 | 29,26,59,57,6,15,40 |
| 14 | 1 | 0 | 45 | 38 |
| 15 | 2 | 0 | 28,6 | 47,34 |
| 16 | 6 | 0 | 1,22,41,14,13,47 | 17,18,47,40,16,57 |
| 17 | 7 | 1 | 55,59,14,60,45,0,33 | 55,3,17,59,53,30,1 |
| 18 | 6 | 0 | 57,7,29,28,50,9 | 21,57,28,43,51,18 |
| 19 | 8 | 1 | 2,31,20,25,10,43,57,2 | 28,9,9,55,18,21,29,20 |
| 20 | 3 | 1 | 57,26,6 | 9,36,42 |

После того как каждый участник фокус-группы завершал двадцатую итерацию по подписанию электронных документов и пытался подписать новый электронный документ, начиналась реализация метода определения события инфомационной безопасности. Из БД по идентификатору подписанта извлекались данные предыдущих операций подписи и преобразовывались в векторы следующего вида:

{9,1,1,41},{9,1,24,56},{9,1,49,57},{9,1,23,53},{9,1,38,58},{9,1,6,4},{9,1,46,22},
{9,1,45,12},{9,1,3,42},{1,0,51,32},{3,1,8,21},{3,1,19,6},{3,1,23,46},{4,0,45,3},{4,0,12,32},
{4,0,34,1},{4,0,39,49},{1,0,52,45},{5,1,32,42},{5,1,55,30},{5,1,3,30},{5,1,26,26},{5,1,34,6},
{4,1,42,20},{4,1,42,24},{4,1,40,23},{4,1,16,4},{2,1,1,18},{2,1,37,26},{2,0,57,20},{2,0,25,18},
{4,0,28,36},{4,0,53,37},{4,0,33,46},{4,0,5,45},{8,1,43,36},{8,1,20,27},{8,1,1,43},{8,1,11,5},
{8,1,36,10},{8,1,39,32},{8,1,52,26},{8,1,2,49},{8,1,10,42},{8,1,4,47},{8,1,49,38},{8,1,23,28},
{8,1,1,53},{8,1,14,2},{8,1,6,37},{8,1,56,23},{7,0,45,29},{7,0,56,26},{7,0,1,59},{7,0,38,57},
{7,0,50,6},{7,0,52,15},{7,0,25,40},{1,0,45,38},{2,0,28,47},{2,0,6,34},{6,0,1,17},{6,0,22,18},
{6,0,41,47},{6,0,14,40},{6,0,13,16},{6,0,47,57},{7,1,55,55},{7,1,59,3},{7,1,14,17},{7,1,60,59},
{7,1,45,53},{7,1,0,30},{7,1,33,1},{6,0,57,21},{6,0,7,57},{6,0,29,28},{6,0,28,43},{6,0,50,51},
{6,0,9,18},{8,1,2,28},{8,1,31,9},{8,1,20,9},{8,1,25,55},{8,1,10,18},{8,1,43,21},{8,1,57,29},
{8,1,2,20},{3,1,57,9},{3,1,26,36},{3,1,6,42}.

В каждом из представленных выше векторов первое значение соответствует количеству подписываемых документов, второе – количеству неверных попыток аутентификации, третье – продолжительности сравнения хэш-значения, четвертое – продолжительности отправки хэш-значения. В группе векторов, соответствующих одной итерации, первое и второе значения будут одинаковы, так как количество подписываемых документов и количество неверных попыток аутентификации формируются в самом начале использования ПАП. После получения групп векторов устанавливается множитель, который необходимо использовать при определении порогового значения для каждого из параметров, значения которых образуют вектор, а также следующие весовые коэффициенты для этих значений:

– количество подписываемых документов – наименьший коэффициент;

– количество неверных попыток аутентификации для доступа к личному ключу пользователя – высокий коэффициент;

– продолжительность сравнения хэш-значения подписываемых документов – средний коэффициент;

– продолжительность отправки хэш-значения подписываемых данных в УСП – высокий коэффициент.

После этого на основе полученных данных вычисляется стандартное отклонение σ по формуле

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(X_i - \overline{X})^2},$$

где $n$ – количество значений в выборке; $X_i$, $\overline{X}$ – отдельное и среднее значения в выборке соответственно.

Вычислив среднее значение каждого параметра и его стандартное отклонение, следует выполнить проверку новых значений на выход за пределы порогового значения каждого параметра путем сравнения текущего значения с суммой среднего значения параметра и произведения коэффициента порога, стандартного отклонения и весового коэффициента. Если значение превышает пороговое, принимается решение о том, что событие является нарушением устойчивости цифрового образа, и это событие помечается как событие информационной безопасности.

Рассмотрим несколько примеров практического использования разработанного метода в СОП, в которых применяется ПАП [4]. Среднее значение, стандартное отклонение и пороговое значение для каждого параметра, используемые в рамках этих примеров, представлены в табл. 2.

**Таблица 2.** Среднее значение, стандартное отклонение и пороговое значение для каждого параметра
**Table 2.** Average value, standard deviation and threshold value for each parameter

| Параметр / Parameter | $\overline{X}$ | σ | Пороговое значение / Threshold value |
|---|---|---|---|
| Количество подписываемых документов | 6,03 | 2,28 | 6,49 |
| Количество неверных попыток аутентификации для доступа к личному ключу пользователя | 0,63 | 0,49 | 1,59 |
| Продолжительность сравнения хэш-значения подписываемых документов | 28,82 | 18,93 | 47,65 |
| Продолжительность отправки хэш-значения подписываемых данных | 30,63 | 16,81 | 64,06 |

*Пример 1.* Входной параметр – вектор {1,3,0,0}. Это свидетельствует о том, что пользователю был отправлен на подпись 1 документ, количество реализованных им неверных попыток аутентификации для доступа к личному ключу – 3. Значение первого параметра не превышает пороговое значение (6,49), поэтому в соответствии с предложенным методом должен быть выполнен анализ значения второго параметра. Данное значение на 55,35 % превышает установленную пороговую величину (1,59). Это свидетельствует о том, что доступ к личному ключу был заблокирован, поскольку было превышено пороговое значение количества попыток аутентификации для доступа к личному ключу пользователя. В таком случае в соответствии с предложенным методом по завершении анализа значения второго параметра СОП и SIEM-системе будет передано сообщение о нарушении цифрового образа.

*Пример 2.* Входной параметр – вектор {10,1,50,120}, т. е. пользователю было отправлено на подпись 10 документов, количество реализованных им неверных попыток аутентификации для доступа к личному ключу – 1. Количество отправленных на подпись документов и количество попыток неверной аутентификации не превышают установленные пороговые значения (6,49 и 1,59 соответственно). Однако продолжительность сравнения хэш-значения подписываемых документов и продолжительность отправки хэш-значения подписываемых данных превышают установленные пороговые значения (47,65 и 64,06 соответственно). В таком случае в соответствии с предложенным методом по завершении анализа значения третьего параметра СОП и SIEM-системе будет передано сообщение о нарушении цифрового образа.

*Пример 3.* Входной параметр – вектор {20,3,0,0}, т. е. пользователю было отправлено на подпись 20 документов, количество реализованных им неверных попыток аутентификации для доступа к личному ключу – 3. Первое значение входного параметра на 208,17 % превышает установленное пороговое значение. В соответствии с предложенным методом по завершении анализа значения первого параметра СОП и SIEM-системе будет передано сообщение о нарушении цифрового образа.

**Заключение**

1. Разработанный метод представляется перспективным для организации процесса анализа событий информационной безопасности системы облачной подписи, в которых предусмотрено применение протокола активации подписи. Это обусловлено тем, что в основу метода заложены механизмы анализа параметров, характеризующих профиль подписанта в указанных системах, за счет чего можно установить, в каких случаях использование указанного протокола является штатным, а в каких «аномальным». Благодаря этому можно обеспечить уменьшение количества ложноположительных и ложноотрицательных результатов анализа событий информационной безопасности в системе облачной подписи.

2. При использовании предлагаемого метода обнаружения событий информационной безопасности обеспечиваются следующие возможности:

– обновление данных о действиях пользователя и перерасчет показателей пороговых значений;

– добавление возможности предоставления сведений при регистрации сведений о деятельности пользователя в системе облачной подписи для уменьшения ошибок при работе метода;

– комбинирование с другими методами обнаружения аномального поведения пользователей.

3. Дальнейшие исследования будут направлены на усовершенствование механизмов обнаружения событий информационной безопасности, на которых основан предложенный метод.

**Список литературы**

1. Герасимов, В. А. Использование системы облачной электронной подписи для организации электронного голосования / В. А. Герасимов, М. А. Казловский // Цифровая трансформация. 2024. Т. 30, № 1. С. 52–62. http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62.
2. Кочин, В. П. Методика создания и структура корпоративного подразделения информационной безопасности / В. П. Кочин, А. В. Шанцов // Цифровая трансформация. 2022. Т. 28, № 3. С. 65–72. http://doi.org/10.35596/2522-9613-2022-28-3-65-72.
3. Апанасевич, М. В. Разработка методики оценки уровня инновационного потенциала промышленного предприятия / М. В. Апанасевич // Цифровая трансформация. 2022. Т. 28, № 2. С. 5–13. http://doi.org/10.35596/2522-9613-2022-28-2-5-13.
4. Performance Evaluation of Machine Learning Algorithms for Intrusion Detection System // Cryptology ePrint Archive. Mode of access: https://eprint.iacr.org/2023/1546. Date of access: 17.12.2023.

**References**

1. Herasimou V. A., Kazlouski M. A. (2024) Using a Cloud-Based Electronic Signature System for Organizing Electronic Voting. *Digital Transformation*. 30 (1), 52–62. http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62 (in Russian).
2. Kochin V. P., Shantsov A. V. (2022) Methodology of Creation and Structure of the Corporate Information Security Unit. *Digital Transformation*. 28 (3), 65–72. http://doi.org/10.35596/2522-9613-2022-28-3-65-72 (in Russian).
3. Apanasevich M. V. (2022) Development of a Methodology for Assessing the Level of Innovative Potential of an Industrial Enterprise. *Digital Transformation*. 28 (2), 5–13. http://doi.org/10.35596/2522-9613-2022-28-2-5-13 (in Russian).
4. Performance Evaluation of Machine Learning Algorithms for Intrusion Detection System. *Cryptology ePrint Archive*. Available: https://eprint.iacr.org/2023/1546 (Accessed 17 December 2023).

**Вклад авторов / Authors' contribution**

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

**Сведения об авторах**

**Герасимов В. А.,** сотр. науч.-исслед. ин-та технической защиты информации, магистрант каф. информационных технологий автоматизированных систем, Белорусский государственный университет информатики и радиоэлектроники

**Бойправ О. В.,** канд. техн. наук, доц., доц. каф. защиты информации, Белорусский государственный университет информатики и радиоэлектроники

**Адрес для корреспонденции**

220088, Республика Беларусь,
г. 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. A.,** Employee of the Research Institute for Technical Information Protection, Master's Student at the Department of Information Technologies of Automated Systems, Belarusian State University of Informatics and Radioelectronics

**Boyprav O. V.,** Cand. of Sci., Associate Professor, Associate Professor at the Information Security Department, Belarusian State University of Informatics and Radioelectronics

**Address for correspondence**

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