УДК 004.056.5 Вестник УрФО № 1(47) / 2023, с. 51–58

Афанасьева С.В., Кузьмина У.В.

DOI: 10.14529/secur230105

ОСНОВНЫЕ ПРОБЛЕМЫ ПРИ РАБОТЕ С ЦЕНТРАМИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время количество киберугроз постоянно увеличивается, а их техники и тактики совершенствуются. Для мониторинга, обнаружения, а также последующего реагирования на инциденты информационной безопасности организации создают Security Operation Center (далее - SOC) или центры мониторинга информационной безопасности. В данной статье рассматриваются важные проблемы, с которыми сталкиваются IT-специалисты при работе с центрами мониторинга информационной безопасности. Подробный анализ этих проблем позволит начинающим специалистам не допускать ошибок при работе с центрами мониторинга информационной безопасности, а для опытных специалистов станет вектором движения при улучшении центров мониторинга.

Ключевые слова: *информационная безопасность, SOC, центр мониторинга информационной безопасности, инцидент информационной безопасности, киберугроза, реагирование на инциденты информационной безопасности.*

Afanaseva S.V., Kuzmina U.V.

MAIN PROBLEMS WORKING WITH SECURITY OPERATION CENTER

Nowadays cyber threats are steadily increasing and their quality is improving in terms of techniques and tactics. To monitor, detect, and subsequently respond to information security incidents, organizations are establishing Security Operation Centers (SOC) or Information Security Monitoring Centers. This article discusses important challenges that IT professionals face when dealing with information security monitoring centers. Understanding these problems will enable newcomers to avoid mistakes when working with information security monitoring centers, and for experienced professionals it will serve as a vector for improving monitoring centers.

Keywords: *information security, SOC, information security monitoring center, information security incident, cyber threat, information security incident response.*

Центром мониторинга информационной безопасности называется подразделение или отдел информационной безопасности (далее - ИБ), в котором на регулярной основе или постоянно выполняется мониторинг событий ИБ, поступающих как от средств защиты информации (далее - СЗИ), так и от других источников информации. Кроме того, базовыми функциями SOC являются реагирование на инциденты ИБ, последующее их расследование и создание рекомендаций по предотвращению инцидента в будущем. SOC состоит из квалифицированных специалистов по информационной безопасности, средств защиты информации и сопутствующих методов, а также из совокупности процессов, объединяющих людей и технологии в противодействии нарушителю ИБ организации.

Предпосылками к созданию SOC являются:

• Требования ФСТЭК России и ФСБ России (Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017), где внедрение SOC является обязательной процедурой;

• Отсутствие организованного постоянного контроля происходящего в инфраструктуре организации;

• Активное развитие инфраструктуры организации, а также ее полная модернизация;

• Не продуманная концепция выбора и установки СЗИ;

• Появление новых угроз и уязвимостей, актуальных для организации.

• Таким образом, внедрение SOC становится процедурой, имеющей рекомендательный характер для каждой организации и обязательной для субъектов критической информационной инфраструктуры.

К основным задачам SOC относится:

• определение ключевых показателей эффективности работы SOC-Центра - критериев KPI (Key Performance Indicators,);

• получение деталей подключения информационных и защитных систем защищаемого объекта организации к инфраструктуре SOC-Центра, а также данных об изменениях конфигурации защищаемого объекта на всех его уровнях;

• выстраивание процессов мониторинга, обнаружения, реагирования на инциденты информационной безопасности;

• повышение состояния защищенности объектов посредством внедрения дополнительных средств и мер защиты;

• постоянное совершенствование работы SOC, например, путем проведения «тренировок» персонала по возможным угрозам (например, фишинговая рассылка).

Между тем с каждым годом методики по созданию SOC пытаются внести новые элементы и усовершенствованные алгоритмы, несмотря на то, что большинство организаций еще не решили текущие проблемы технического, программного и нормативно-правового характера. Ниже будут рассмотрены и кратко описаны основные проблемы, с которыми сталкиваются специалисты при создании и обслуживании центров мониторинга информационной безопасности.

1. Выбор модели развертывания SOC: внешний или внутренний.

Существует два способа развертывания центра мониторинга ИБ: непосредственно в контуре предприятия (внутренний) и SOC на аутсорсинге (внешний) [6]. Ниже в таблице представлены основные преимущества и недостатки при выборе модели развертывания SOC.

Кроме того, с недавних пор применяют гибридный способ, когда создается внутренний SOC, в котором работает несколько человек и следит за тем, что выполняет внешний SOC. В свою очередь, основные обязанности по мониторингу, обнаружению и реагированию на события ИБ выполняет именно внешний SOC.

В выборе модели развертывания SOC стоит учитывать потребности организации, ее потенциал, штат сотрудников и их компетенции, наличие СЗИ и сопутствующего оборудования. Дополнительно стоит провести анализ в области сервис-провайдеров, оценить финансовые возможности организации.

При оценке SOC на аутсорсинге стоит начать с проверки наличия сертификатов ФСТЭК России на деятельность по мониторингу, ФСБ России на работу со средствами криптозащиты, заключенного согласия с НКЦКИ. Далее стоит провести собеседование с компанией, предоставляющей услугу, и оценить ожидания организации на возможности компании. В качестве дополнительного шага можно запросить рецензию клиентов этой компании.

2. Распределение задач в SOC

Каждая организация использует свой подход в распределении задач для сотрудников SOC. Стоит выделить три основных подхода распределения задач: разделение по

Таблица 1

Преимущества и недостатки при выборе модели развертывания SOC

Модель развертывания	Преимущества	Недостатки
Внешний SOC	• Не нужно нанимать квалифицированный персонал; • Режим 24/7 будет поддерживать аутсорсинговая компания, а не штат организации; • На базе методик и стандартов аутсорсиноговой компании будут активнее запускаться процессы, реализуемые SOC; • Более низкие финансовые затраты, чем при построении внутреннего SOC; • Обработка и хранение событий ИБ в инфраструктуре исполнителя; • Экономия на содержании технических компонентов и обслуживающем персонале; • Организация может сосредоточить внимание на своих основных бизнес-процессах.	• Высокие требования к каналам между площадками заказчика и исполнителя, так как для обработки передается большой поток данных; • Необходимо потратить время на анализ бизнес-проблем организации и внедрить сквозные процессы с участием внутренних и внешних сотрудников; • Данные хранятся и анализируются за пределами периметра организации, появляются дополнительные риски, связанные с утечкой информации.
Внутренний SOC	• Данные хранятся и обрабатываются внутри периметра согласно всем внутренним требованиям организации; • Внутренние сотрудники лучше знают инфраструктуру организации, а также все «подводные» камни; • Есть постоянный доступ к данным (в случае отсутствия Интернета со внешнего SOC нельзя будет использовать данные).	• Дефицит квалифицированного персонала; • Закупка дорогостоящих компонентов SOC; • Несовместимость средств защиты информации в результате неправильной настройки; • Построение может занять годы и не всегда гарантирует результат.

уровню квалификации и ответственности, по векторам атак или видам угроз, по очередности [5].

Первый подход заключается в выделении нескольких линий с различными компетентностями сотрудников: первая линия обрабатывает все поступающие события и по мере сил с ними справляется. Если инцидент является более сложным, то он отправляется ко второй линии, где сотрудники обладают большим опытом и навыками работы с усложненными ситуациями. Соответственно, если сотрудники второй линии не справляются с инцидентом, то ему назначается статус «критический» и переход осуществляется к третьей линии, где сотрудники являются узконаправленными специалистами в таких областях, как угрозы операционных систем, сетевые угрозы, угрозы отказа в обслуживании и т.д.

Преимуществом данного подхода несомненно является накопление опыта и практики для сотрудников первой линии, совершенствование знаний и навыков для сотрудников второй и третьей линий. Недостатком является огромный объем работ при подготовке инструкций по реагированию на инциденты ИБ для всех линий сотрудников SOC.

Второй подход подразумевает разделение специалистов по разным векторам атак или видам угроз, на которых они специализируются (например, вредоносное программное обеспечение, фишинг, сетевые атаки и т.д.). Кроме того, разделение может осуществляться по типам систем (автоматизированные рабочие места, специализированные приложения, центр обработки данных и т.д.) или по степени важности систем (инциденты, относящиеся к критически важным системам, сразу переходят ко второй линии).

Отрицательной чертой данного подхода может быть незаменимость сотрудников, работающих в определенной области, а положительной – возможность для сотрудника сфокусироваться на интересной ему области и наращивать потенциал в выбранном направлении.

Третий подход реализует «живую» очередь из инцидентов ИБ, в которой сотрудники способны справляться с инцидентом без пере-

дачи его к более сильному специалисту. При этом первой линией в данном подходе может выступать искусственный интеллект, который убирает лишнюю информацию в виде ложных срабатываний и передает дальнейшие сведения единому фронту сотрудников SOC.

Такой подход, в отличии от предыдущего, позволяет сотрудникам работать со всеми типами инцидентов, тем самым повышая их знания в различных областях. Тогда проблемой становится поиск квалифицированных сотрудников, способных справится со всевозможными инцидентами ИБ.

При выборе подхода стоит руководствоваться квалификацией сотрудников и их наличием в SOC. Кроме того, можно заметить, что подходы возможно объединять между собой, получая при этом гибридный вариант, который в свою очередь может стать подходящим для организации.

3. Инструментарий SOC

Базовым инструментом для каждого SOC принято считать Security Information and Event Management (далее - SIEM). Но просто установка SIEM не позволит в полной мере исполнять основные задачи SOC. Ниже приведены основные инструменты, которые могут быть внедрены в SOC, и примеры продуктов отечественного и зарубежного рынка. Некоторые из них входят в состав других, но так или иначе являются отдельными инструментами SOC.

Исследовательская компания Gartner считает, что базой каждого SOC является

Таблица 2

Инструментарий SOC

Инструмент	Пример
Security Information and Event Management (SIEM)	Ankey SIEM, MaxPatrol SIEM, RuSIEM, КОМРАД, SearchInform SIEM
Endpoint Detection and Response (EDR)/ Extended Detection and Response (XDR)	Kaspersky EDR, Positive Technologies XDR, Managed XDR Group-IB
Network Traffic Analysis (NTA)/ Network Detection and Response (NDR)	Positive Technologies Network Attack Discovery, Group-IB Threat Detection System, Kaspersky Anti Targeted Attack, «Гарда Монитор»
Incident Response Platform (IRP)/ Security Orchestration, Automation and Response (SOAR)	Jet Signal, R-Vision Incident Response Platform, Security Vision Incident Response Platform
Threat Intelligence Platform (TIP)	Group-IB TI, Kaspersky TI, PT Cybersecurity Intelligence, R-Vision TIP
Intrusion Detection System (IPS)/ Intrusion Prevention System (IDS)	Traffic Inspector Next Generation, ViPNet IDS 3, «Аргус», «СОВ Континент», «Рубикон», «С-Терра СОВ»
Managed Detection and Response (MDR)	Group-IB MDR Services, Kaspersky MDR, Positive Technologies Expert Security Center
Сервисы для анализа поведения пользователей	InfoWatch Prediction, SearchInform ProfileCenter
Средства контроля и анализа защищенности	RedCheck, XSPIDER, Сканер-ВС, Ревизор сети
Технологии хранения данных и резервного копирования	Эльбрус-2000, Норси-Транс, Aerodisk, DEPO, RCNTEC, RuBackup, Handy Backup
Сервисы по форензике	Elcomsoft Premium Forensic Bundle, ePlat4m Security GRC, EtherSensor

«SIEM + NTA + EDR» [4]. Для обогащения данной комбинации, а также для повышения эффективности работы SOC следует рассмотреть следующие инструменты: IRP/SOAR решения, сервисы TIP, IPS/IDS, средства контроля и анализа защищенности, технологии хранения данных и резервного копирования, MDR, сервисы для анализа поведения пользователей, сервисы по форензике.

4. Процесс управления жизненным циклом инцидента

Управление инцидентами ИБ является одним из важнейших процессов, реализуемых в SOC [1]. Если хотя бы на одном из этапов возникнут сложности, это может привести к полному провалу всего процесса, что является недопустимым. На рис. 1 приведены этапы реагирования на инцидент ИБ и их описание.

Для начала необходимо рассмотреть отечественные и иностранные стандарты, такие как:

Рис. 1. Этапы реагирования на инцидент

• National Institute of Standards and Technology. NIST SP 800-61;

• Carnegie Mellon University. CMU/SEI-2018-TR-007;

• Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 «Менеджмент инцидентов информационной безопасности»;

• РС БР ИББС-2.5-2014 «Менеджмент инцидентов ИБ»;

• ENISA «Руководство по эффективной практике для управления инцидентами».

Стандарты в полной мере определяют жизненный цикл инцидента, роли и область ответственности в данном процессе, ключевые показатели эффективности, рекомендации по управлению инцидентами. Но даже при наличии обширной теории, на практике вопросы и проблемы все равно возникают:

• Организация работает только с реагированием – из-за этого невозможно полностью видеть картину происходящего;

• Неточные или неполные сценарии для реагирования на определенный инцидент – время реагирования на инцидент увеличивается из-за задержки на получение точных указаний;

• Нет улучшения процесса управления инцидентом – без совершенствования процесса невозможно предотвратить актуальные угрозы и уязвимости.

5. Показатели эффективности SOC

Оценка эффективности SOC является значимым параметром на пути развития информационной безопасности в организации. Без этого организация не сможет вовремя обнаружить и исправить актуальные угрозы, что в свою очередь ведет к потери ключевой информации для бизнеса [9].

При создании или подключении SOC на начальном этапе должно прописываться соглашение об уровне услуг (Service Level Agreement, SLA) – договор, внутри подразде-

ления или между клиентом и заказчиком, в котором содержатся описание услуги, обязанности сторон, а также уровень качества предоставления данной услуги. В нем присутствуют базовые метрики, такие как время реагирования на инцидент, количество ложных срабатываний, время оповещения персонала, скорость обработки инцидента и т.п. Более того, не стоит забывать про основной ключевой показатель эффективности (Key Performance Indicator, KPI) для любого SOC – недопущение инцидентов, приносящих ущерб организации. Чтобы убедиться в эффективности работы SOC, стоит провести тренировку, которая имитирует реальные угрозы.

6. Определение основных источников информации для SOC

Для эффективной работы SOC необходимо обеспечить сотрудников актуальной информацией, касающейся инфраструктуры организации, изменениях в ней. Кроме того, постоянно должна отслеживаться информация о новых угрозах и уязвимостях [2]. Условно источники информации можно разделить на внутренние и внешние. Ниже приведены основные источники информации для SOC.

В данной таблице представлен основной

Таблица 3

Основные источники информации

Внутренние источники информации	Внешние источники информации
События безопасности с инфраструктурных компонентов (операционные системы, автоматизированные системы оповещения, прикладное программное обеспечение и др.)	Информация от ведомственных и корпоративных центров в рамках соглашений по информационному обмену (ФСТЭК России, ФСБ России, ЦБ России)
События со средств защиты информации (антивирус, межсетевой экран, NTA, EDR и др.)	Сообщества в социальных сетях, форумы в Интернете или Даркнете
Актуальные данные об активах (база данных управления конфигурацией, таблицы маршрутизации и др.)	Информация о новых инструментах (средствах защиты информации) от вендоров
Дополнительная информация от внутренних сотрудников	Данные об угрозах и уязвимостях (Threat Intelligence, Open Source Intelligence и др.)

объем источников информации для SOC. При выборе источника стоит руководствоваться наличием тех или иных средств защиты информации, а также заинтересованностью сотрудников в поиске актуальной информации, касающейся новых угроз и уязвимостей [10].

7. Организационная структура SOC

Корректно сформированная команда специалистов является одним из важных показателей для эффективной работы SOC [3]. Ниже представлена организационная структура SOC (рис. 2).

Одна из важнейших групп для любого SOC – это группа мониторинга и реагирования, которая выполняет первостепенные задачи SOC, описанные в начале статьи. В зави-

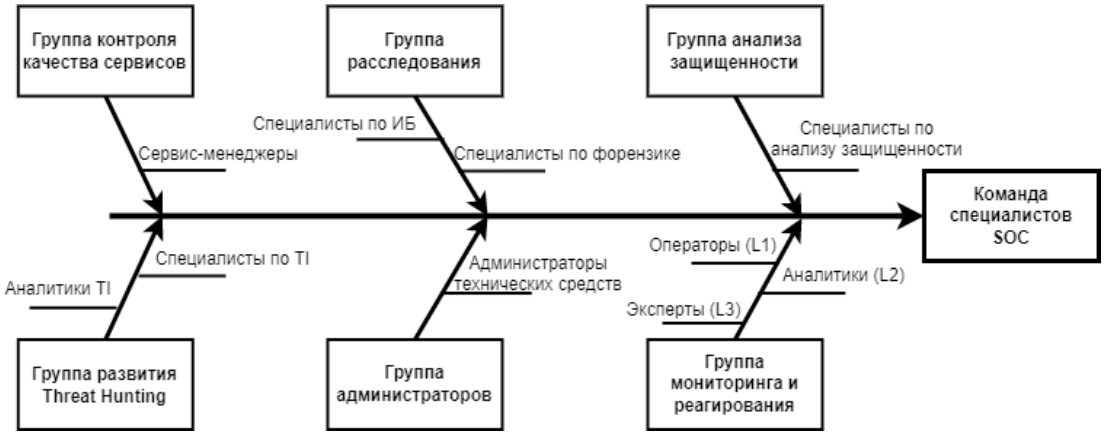

Рис. 2. Организационная структура SOC

симости от выбора подхода распределения задач в SOC может состоять из операторов, аналитиков и экспертов, распределенных по нескольким линиям. Операторы выполняют первичную фильтрацию событий ИБ, полученных от различных источников, регистрируют инциденты ИБ, выполняют действия, изложенные в инструкции по реагированию на инциденты, соответствующие первой линии. Аналитики проводят анализ инцидентов или поступающих угроз, прогнозируют их развитие, создают превентивные меры, а также могут активно участвовать в реагировании на инцидент ИБ на любом из его этапов. В свою очередь, эксперты являются узконаправленными специалистами в области ИБ, которые совершенствуют базу знаний всего SOC. Более того, эксперты также участвуют в работе операторов и аналитиков, например, в случае, если инцидент является критическим [7].

Группа администраторов, состоящая из администраторов технических средств, выполняет работы, относящиеся к программно-аппаратным средствам, СЗИ, сетевым техническим средствам и т.д. Специалисты из группы развития Threat Hunting собирают информацию об актуальных угрозах, новых уязвимостях, занимаются разработкой мер по защите от угроз или нарушителей, проверяют информацию из внешних источников данных. Группа контроля качества сервиса отвечает за выполнение и соблюдение SLA, в том числе за организацию всех процессов взаимодействия. Специалисты из группы расследования должны собрать и зафиксировать всю информацию, касающуюся инцидента, проанализировать весь объем данных, определить какой вред получила организация от инцидента и принять меры в отношении виновных лиц. Группа анализа защищенности отвечает за тестирование систем на проникновение, анализ рисков ИБ в SOC, состояние защищенности как организации, так и самого SOC.

Безусловно исходить нужно от размеров SOC и численности команды. Опираться необходимо на функции, который SOC организации должен исполнять. После этого необходимо выбрать группы, которые войдут в состав SOC. Для каждой группы должны быть определены руководители, распределена ответственность, основные должностные обязанности [8].

В данной статье проанализированы основные проблемы, с которыми сталкиваются специалисты ИБ при работе с центрами мониторинга информационной безопасности, а также подобно представлены возможные варианты решения данных проблем. Кроме того, даны базовые рекомендации для принятия оптимальных решений в тех или иных случаях.

Проведенный анализ позволяет сделать вывод, что для решения описанных проблем необходимо создание общих стандартов и методик, которые бы регламентировали процесс создания SOC, введение в эксплуатацию и дальнейшую работу. Эти документы должны быть одобрены федеральными органами исполнительной власти, такими как ФСТЭК России и ФСБ России.

Более того, необходимо аккумулировать опыт ведущих отечественных компаний ИБ для создания центров мониторинга ИБ следующего поколения: SOC с полной автоматизацией деятельности человека на этапе мониторинга и реагирования, а также четко выстроенной организационной структурой. В этом случае может получиться действительно эффективный инструмент, который будет защищать организацию от новых угроз современного мира.

Литература

1. Энсон С. Реагирование на компьютерные инциденты. // Wiley, 2021. 436 с.

2. Калугина О., Баранкова И., Михайлова У. Разработка инструмента моделирования угроз безопасности информационной системы предприятия // 2nd ICECCE 2020. 2. 2020. С. 1–5.

3. Ройс Д. Искусство тестирования на проникновение в сеть // Manning Shelter Island, 2021. 312 с.

4. Васильева И.Н. Расследование инцидентов информационной безопасности // Издательство СПбГЭУ, 2019. 113 с.

5. Солдатов С. Организация работы и обработка уведомлений в SOC // Лаборатория Касперского, 2022. URL: https://www.kaspersky.ru/blog/soc-alert-processing/33948/.

6. Натанс Д. Проектирование и строительство SOC // Syngress, 2014. 276 с.

7. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Формирование компетенций специалиста по ин-

формационной безопасности // Актуальные проблемы современной науки, техники и образования: тезисы докладов 77-й международной научно-технической конференции. 2019. С. 428.

8. Анисимова А.А. Менеджмент в сфере информационной безопасности. // Национальный Открытый Университет "ИНТУИТ", 2016. 213 с.

9. Дронова Г.А. Управление информационной безопасностью // Новосибирск: НГТУ, 2016. 28 с.

10. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 217–220.

References

1. Enson S. Reagirovaniye na komp'yuternyye intsidenty. // Wiley, 2021. 436 s.

2. Kalugina O., Barankova I., Mikhaylova U. Razrabotka instrumenta modelirovaniya ugroz bezopasnosti informatsionnoy sistemy predpriyatiya // 2nd ICECCE 2020. 2. 2020. S. 1–5.

3. Roys D. Iskusstvo testirovaniya na proniknoveniye v set' // Manning Shelter Island, 2021. 312 s.

4. Vasil'yeva I.N. Rassledovaniye intsidentov informatsionnoy bezopasnosti // Izdatel'stvo SPbGEU, 2019. 113 s.

5. Soldatov S. Organizatsiya raboty i obrabotka uvedomleniy v SOC // Laboratoriya Kasperskogo, 2022. URL: https://www.kaspersky.ru/blog/soc-alert-processing/33948/.

6. Natans D. Proyektirovaniye i stroitel'stvo SOC // Syngress, 2014. 276 s.

7. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Formirovaniye kompetentsiy spetsialista po informatsionnoy bezopasnosti // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya: tezisy dokladov 77-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2019. S. 428.

8. Anisimova A.A. Menedzhment v sfere informatsionnoy bezopasnosti. // Natsional'nyy Otkrytyy Universitet "INTUIT", 2016. 213 s.

9. Dronova G.A. Upravleniye informatsionnoy bezopasnost'yu // Novosibirsk: NGTU, 2016. 28 s.

10. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Prognozirovaniye lokal'nykh i vneshnikh ugroz na informatsionnyye servery predpriyatiya // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2017. T. 1. S. 217–220.

АФАНАСЬЕВА Светлана Викторовна, студент 5 курса кафедры Информатики и Информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. Россия, 455000, г. Магнитогорск, пр. Ленина 38. E-mail: afasvetlana0@gmail.com

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной безопасности, Магнитогорский государственный технический университет им. Г.И. Носова. Россия, 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

AFANASEVA Svetlana Viktorovna, 5th year student of the Department of Informatics and Information, Security of Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: afasvetlana0@gmail.com

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information, Security of Nosov Magnitogorsk State Technical University. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: ylianapost@gmail.com