УДК 004.056 DOI: 10.26102/2310-6018/2021.32.1.020

Система управления данными кибербразведки

А.М. Вульфин
ФГБОУ ВО «Уфимский государственный авиационный технический университет»
Уфа, Российская Федерация

Резюме. В данной статье рассматривается проблема повышения оперативности распространения информации о новых угрозах. Традиционные методы обмена информацией об инцидентах информационной безопасности (ИБ) практически не масштабируемы и с ростом числа инцидентов перестают справляться со своей задачей. Существенно возрастает нагрузка на специалистов, занимающихся мониторингом состояния информационной системы, а эффективность их работы снижается. Целью исследования является повышение эффективности центра мониторинга и реагирования на инциденты информационной безопасности за счет развертывания программной платформы управления данными кибербразведки. Объект исследования – центр мониторинга и реагирования на инциденты ИБ, предмет исследования – система управления данными кибербразведки. Проанализированы подходы к реализации кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ, выполнен обзор функциональных возможностей существующих решений, разработан план развертывания платформы кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ организации. Основные этапы развертывания включают подготовительную работу, установку, настройку и тестирование платформы. Эффективность функционирования центра мониторинга и реагирования на инциденты ИБ после внедрения платформы выросла на 41,7 %, а уровень зрелости повысился с «начального» до «базового».

Ключевые слова: кибербразведка, центр мониторинга и реагирования на инциденты ИБ, платформа кибербразведки, система управления данными кибербразведки.

Для цитирования: Вульфин А.М. Система управления данными кибербразведки. *Моделирование, оптимизация и информационные технологии.* 2021;9(1). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=925 DOI: 10.26102/2310-6018/2021.32.1.020

Cyber Threat Intelligence Data Management System

A.M. Vulfin
Ufa State Aviation Technical University, Ufa, Russian Federation

Abstract: This article discusses the problem of increasing the speed of disseminating information about new threats. Traditional methods of sharing information about information security (IS) incidents are practically not scalable, and as the number of incidents grows, they fail to cope with their task. The workload of specialists involved in monitoring the state of the information system increases significantly, and the effectiveness of their work decreases. The research aim is the information security incident monitoring and response center efficiency improvement by deploying a software platform for cyber intelligence data management. The object of the study is the IS incident monitoring and response center, the subject of the study is the cyber intelligence data management system. The approaches to the realization of cyber intelligence as a part of IS incident monitoring and response center were analyzed, the functional capabilities of existing solutions were reviewed. The plan for deployment of cyber intelligence platform as a part of an organization IS incident monitoring and response center was developed. The main stages of deployment include preparatory work, installation, configuration, and testing of the platform. After implementing the platform, the performance of the IS incident monitoring and response center increased by 41.7 percent, and the level of maturity increased from " initial " to "basic."

Keywords: cyber intelligence, IS incident monitoring and response center, cyber intelligence platform, Cyber Intelligence Data Management System

For citation: Vulfin A.M. Cyber Threat Intelligence Data Management System. *Modeling, Optimization and Information Technology*. 2021;9(1). Available from: https://moitvivt.ru/ru/journal/pdf?id=925 DOI: 10.26102/2310-6018/2021.32.1.020 (In Russ).

Введение

Аналитики и специалисты по информационной безопасности сталкиваются со все возрастающим количеством киберугроз. Крупные компании неохотно раскрывают сведения об атаках на их инфраструктуру и не публикуют новые методы противодействия. Киберпреступники, наоборот, тщательно и сообща планируют свои атаки и активно делятся уязвимостями и вредоносным ПО. Проблема неосведомлённости о новых угрозах присутствует даже в пределах одной компании, например, в крупных или территориально распределенных организациях. Традиционные методы обмена информацией об инцидентах информационной безопасности, такие как: электронная почта, мессенджеры – не масштабируемы и с незначительным ростом числа инцидентов перестают справляться со своей задачей. Существенно возрастает нагрузка на специалистов, занимающихся мониторингом состояния информационной системы, а эффективность их работы снижается.

Для решения этой проблемы внедряется процесс кибербразведки, или разведки киберугроз (Treat Intelligence, TI). Системы управления данными кибербразведки (СУДК) служат для автоматизации этого процесса. СУДК осведомляют о новых угрозах и атаках, о новых методах злоумышленников ещё до того, как компании будет причинён какой-либо ущерб. Данные для СУДК могут поступать из различных источников, в числе которых: антивирусные базы, центры мониторинга, закрытые сообщества хакеров и объединения по борьбе с киберпреступностью.

Целью исследования является повышение эффективности центра мониторинга и реагирования на инциденты ИБ за счет развертывания программной платформы СУДК Malware Information Sharing Platform (MISP).

Для достижения цели были решены следующие задачи:

- анализ подходов к реализации кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ;
- разработка плана развертывания платформы кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ;
- развертывание и оценка эффективности функционирования платформы кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ.

Анализ процесса кибербразведки в составе центра мониторинга и реагирования на инциденты ИБ

Для выявления целевых атак (APT) на информационные системы необходим анализ значительного объёма входящего и исходящего сетевого трафика и потока событий информационной безопасности для выявления аномальной активности, анализа вектора атаки и оценки возможного ущерба. Для решения подобных задач применяется комплексный подход – создание центра мониторинга и реагирования на инциденты ИБ (Security Operation Center, далее – SOC). Обобщая родственные понятия (команда

реагирования на инциденты компьютерной безопасности (CSIRT), центр обеспечения кибербезопасности (CSOC) и т.п.) [1-7], можно определить SOC как команду аналитиков информационной безопасности, организованную для обнаружения, анализа и реагирования на инциденты информационной безопасности [8], их предотвращение и составление отчетности. Основной целью управления инцидентами ИБ является обеспечение непрерывного мониторинга событий информационной безопасности, своевременное реагирование на инциденты, устранение последствий и формирование выводов для предотвращения возникновения инцидентов в будущем.

Основные задачи и функции SOC, согласно [1-7], представлены в Таблице 1.

Компания Gartner Inc. определяет киберразведку, или разведку киберугроз (Treat Intelligence, TI) как «совокупность знаний, построенных на наблюдениях, включающая в себя контекст, механизмы, индикаторы, последствия и практические рекомендации о существующей или возможной угрозе» [9-10].

Таблица 1 – Основные функции и задачи SOC
Table 1 – Main functions and tasks of the SOC

Функция	**Декомпозиция**	**Инструменты, цель, результаты**
Инвентаризация инфраструктуры и контроль ее состояния	– мониторинг ИТ-инфраструктуры, оборудования, контроль информационных систем, выявление связей между элементами (контроль новых программ, выявление запрещенных программных обеспечений); – составление списка программного и аппаратного обеспечения инфраструктуры КИС и определение их ценности; – контроль учетных записей пользователей, управление доступом; – контроль уязвимостей.	антивирусы, сканеры уязвимости и т. п.
		– выявить наиболее чувствительные информационные ресурсы; – определить ответственных специалистов.
		Схемы, карты, графы ресурсов корпоративной информационной системы (КИС)
Управление уязвимостями	– обнаружение и регистрация в соответствии с типом и уровнем важности, – назначением специалистов и сроков реагирования, – исключение ложноположительных срабатываний	
Консолидация информации об инцидентах ИБ	– выявление инцидентов (данные собираются в центре из различных источников и датчиков, классифицируются и анализируются); – реагирование (назначение ответственных, сроков и алгоритма реагирования);	– электронная почта, – API и др.
		наполнение центральной БД информацией об инцидентах ИБ

	– расследование (определение причин и обстоятельств); – анализ и статистика (накопление статистических данных и реляционный анализ); – построение отчетности.	единая база об инцидентах ИБ (уровни критичности и ущерба, источник события ИБ, статус, вероятность повторения, важность)
Координация и автоматизация реагирования на инциденты ИБ	– первоочередные действия (блокирование угрозы и проверка систем) – расследование и восстановление (сбор свидетельств и восстановление из резервной копии) – эскалация и уведомление (директор по ИБ и директор подразделения)	разработка регламента проведения мероприятий по реагированию на типовые инциденты ИБ
		модуль-конструктор для задания: правил сбора информации, критериев, прав доступа и назначения ответственных лиц
Интеграция с внешними источниками и обмен данными об угрозах		сообщения из SIEM, DLP-систем, антивирусных программ, сканеров уязвимости и т. д.
Сбор показателей эффективности системы защиты (метрик)	– среднее время реагирования на инцидент; – количество инцидентов в работе; – среднее время закрытия инцидента; – отношение закрытых инцидентов к зарегистрированным инцидентам.	Интегральное представление отчетности по типам инцидентов, срокам реагирования и по величине ущерба.

Процесс кибербразведки включает 5 основных этапов [11] (Рисунок 1).

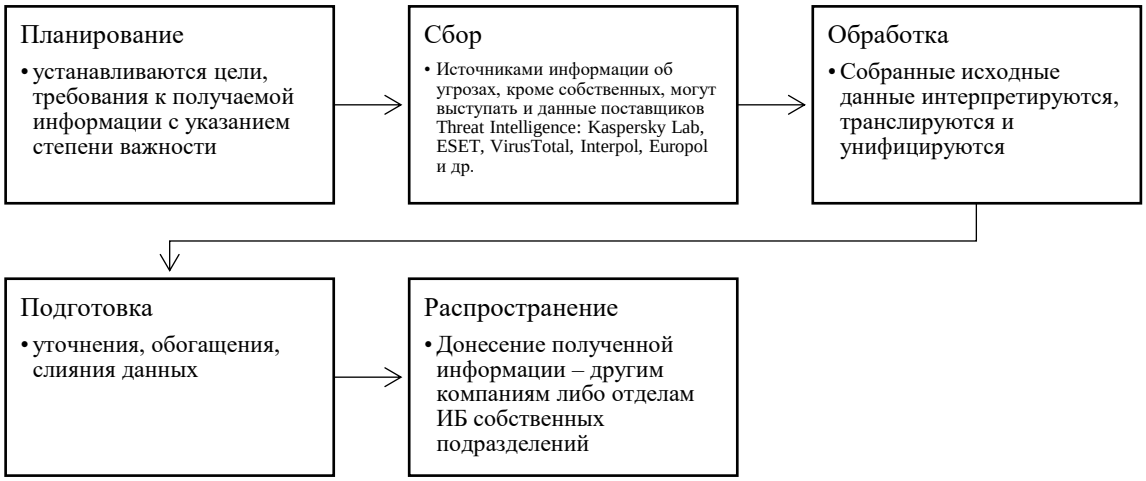

Рисунок 1 – Основные этапы процесса кибербразведки
Figure 1 – The main stages of the treat intelligence process

Т.о., данные кибербразведки – это актуальные сведения об атаках, тактике и технике злоумышленников и индикаторах компрометации (Indicator of Compromise, IoC). Наиболее распространённые индикаторы включают:

– IP-адреса, URL-адреса и доменные имена;

– адреса электронной почты, темы письма, ссылки и вложения;

– ключи реестра, имена файлов и хеши файлов и DLL библиотеки.

Источниками или каналами (feed) кибербразведки являются: антивирусные базы, центры мониторинга, Honeynet-ловушки, закрытые сообщества хакеров, объединения по борьбе с киберпреступностью, Europol, Interpol и базы силовых структур. Инциденты безопасности, зарегистрированные в СУДК под идентификационным номером, называются событиями (event).

Т.о., основные функции СУДК:

– консолидация индикаторов угроз от множества каналов (источников);

– нормализация, обогащение полученных данных, присвоение уровней критичности;

– анализ угроз, векторов атак, и обмен информацией о них;

– анализ поступающих из источников (например, SIEM) событий;

– интеграция с существующими средствами защиты информации.

Системы управления данными кибербразведки функционируют совместно с системами обнаружения и предотвращения вторжений (IDS/IPS) и SIEM-системами. Сравнительный анализ существующих СУДК [9-13] представлен в Таблицах 2 и 3.

Таблица 2 – Сравнительный анализ существующих СУДК
Table 2 – Comparative analysis of existing cyber threat intelligence platform

№	Платформа	Особенности	Достоинства
1	R-Vision Threat Intelligence Platform (г. Москва)	централизованный сбор данных кибербразведки, обработка, анализ взаимосвязей, обогащение индикаторов, выгрузка на средства защиты, поиск и обнаружение в инфраструктуре и автоматизация сценариев	непрерывный сбор, нормализация и хранение информации из различных каналов в базе, что упрощает работу с данными кибербразведки; непрерывный мониторинг индикаторов (syslog, SIEM), что облегчает обнаружение скрытых угроз; быстрый поиск в доступных каналах кибербразведки и автоматизация основных сценариев работы; автоматическая транспортировка обработанных данных средствам защиты информации, что позволяет блокировать угрозы на начальном этапе и минимизировать потери.
2	ThreatStream и Enterprise, компания Anomali	ThreatStream осуществляет оперативную обработку данных об угрозах и объединяет все инструменты в инфраструктуре безопасности, ускоряя обнаружение	ускорение обнаружения угроз на основе объединения существующих решений по обеспечению безопасности в одной системе;

	(США, Калифорния)	угроз и обеспечивая превентивную защиту Индикаторы компрометации могут управляться в рамках платформы и передаваться в другие системы для блокировки и мониторинга. Возможные интеграции: SIEM-системы: межсетевые экраны, IDS, Endpoint, API.	предоставление инструментов для оперативной реализации анализа угроз. автоматизация большинства задач анализа;
3	EclecticIQ Platform	объединяет и интерпретирует данные киберразведки из открытых источников, коммерческих поставщиков и отраслевых партнерств	двухсторонняя интеграция с SIEM для выявления совпадений по базе угроз; возможность построения графа связей объектов feed'ов и внутренних артефактов; передача информации о потенциальных угрозах в SIEM, IPS (Snort, Suricata и др.). Интеграция: AlienVault Open Threat Exchange, Amazon S3, BFK, Binary Defense , Artillery, BitSight Anubis Cyberfeeds, CAPEC, Censys, CIRCL Passive SSL и т.п.
4	ThreatConnect	возможность помещать данные безопасности в контекст киберразведки и аналитики, устанавливать согласованность процессов с указаниями, рабочими процессами и централизованной системой учета, а также измерять эффективность с помощью кроссплатформенной аналитики и настраиваемых панелей мониторинга	автоматизация сбора информации с платформ сбора информации об угрозах ThreatConnect, централизация, агрегация и управление данными киберразведки независимо от источника; Интеграция инструментами SIEM, EDR и брандмауэр позволяет извлекать внутренне созданные журналы в ThreatConnect для дальнейшего обогащения
5	ThreatQuotinet	приоритизация угроз на основании параметров «веса» угроз; авто-настройка внутренней библиотеки угроз на основании «веса» угроз; построение графа связей объектов каналов и внутренних элементов.	ориентированный на угрозы подход к операциям по обеспечению безопасности позволяет устанавливать приоритеты на основе угроз и рисков, сотрудничать между командами, автоматизировать действия и рабочие процессы и интегрировать точечные продукты в единую инфраструктуру безопасности Открытая биржа ThreatQ (модули пользовательской интеграции) обеспечивает самый большой и наиболее

			адаптируемый набор интеграций в отрасли.
6	Your Everyday Threat Intelligence (YETI)	Платформа для организации наблюдаемых объектов, индикаторов компрометации, TTP и знаний об угрозах в едином, унифицированном репозитории; автоматически обогащает события (например, разрешающие домены, география IP); предоставляет пользовательский интерфейс для специалистов на основе Bootstrap и веб-API межмашинного взаимодействия	поддержка основных способов получения данных (источники); интеграция с внутренними системами информационной безопасности по API; обогащение данных и подключение дополнительных внешних сервисов через API; построения графа связей объектов.
7	Malware Information Sharing Platform (MISP)	Простота обмена данными между различными организациями или потоками данных. Функциональность провайдера данных кибербразведки – совместное использование, где каждый может быть потребителем и/или производителем/провайдером; интегрируется с большим количеством каналов кибербразведки через разработанные сообществом плагины интеграции.	поддержка всех известных и используемых форматов импорта и экспорта; визуализация графами, обогащение и классификация инцидентов; многочисленное сообщество профессионалов, множество обучающих материалов, книга по использованию, установке, настройке и администрированию; ежемесячные обновления и поддержка разработчиков.

Результаты анализа существующих решений класса Threat Intelligence обобщены в Таблицу 3.

Таблица 3 – Критерии сравнения платформа СУДК
Table 3 – Cyber Threat Intelligence Platform Comparison Criteria

№	Платформа Критерий	R-Vision Threat Intelligence Platform	ThreatStream и Enterprise, компания Anomali	Eclectic IQ Platform	ThreatConnect	ThreatQuotinet	YETI	MISP
1	Собственные feed-поставщики/аналитические центры предобработки feed	-	+	-	+	+	-	-
2	Количество feed-поставщиков из коробки	0-20	100+	20-100	100+	100+	20-100	20-100
3	Поддерживаемые способы получения feed							
3.1	HTTP-feed	+	+	+	+	-	+	+
3.2	email-feed	-	+	+	+	+	-	+
3.3	Неструктурированные текстовые данные	-	+	-	+	+	-	+

4	Поиск совпадений в событиях SIEM	+	+	+	+	+	-	-
5	Прямое реагирование на инциденты путем интеграции со сторонними системами ИБ	+	+	+	+	-	-	+
6	Реагирование на инциденты с использованием сложных алгоритмов (playbook)	-	-	-	+	-	-	-
7	Ручная настройка параметров «веса» для feed	-	+	-	-	+	-	-
8	Встроенные обсуждения для аналитиков	-	+	+	-	+	+	+
9	Встроенные обсуждения для аналитиков	-	-	+				
10	Дата создания	2019	2014	2017	2012	2018	2018	2011

Рынок платформ кибербразведки возник и развивался в последнее десятилетие в связи с ограниченными возможностями традиционных средств защиты информации в задачах обработки нарастающего потока событий и инцидентов информационной безопасности.

Разработка системы управления данными кибербразведки

Мониторинг КИС организации реализован на основе взаимодействия с удаленным SOC (Рисунок 2).

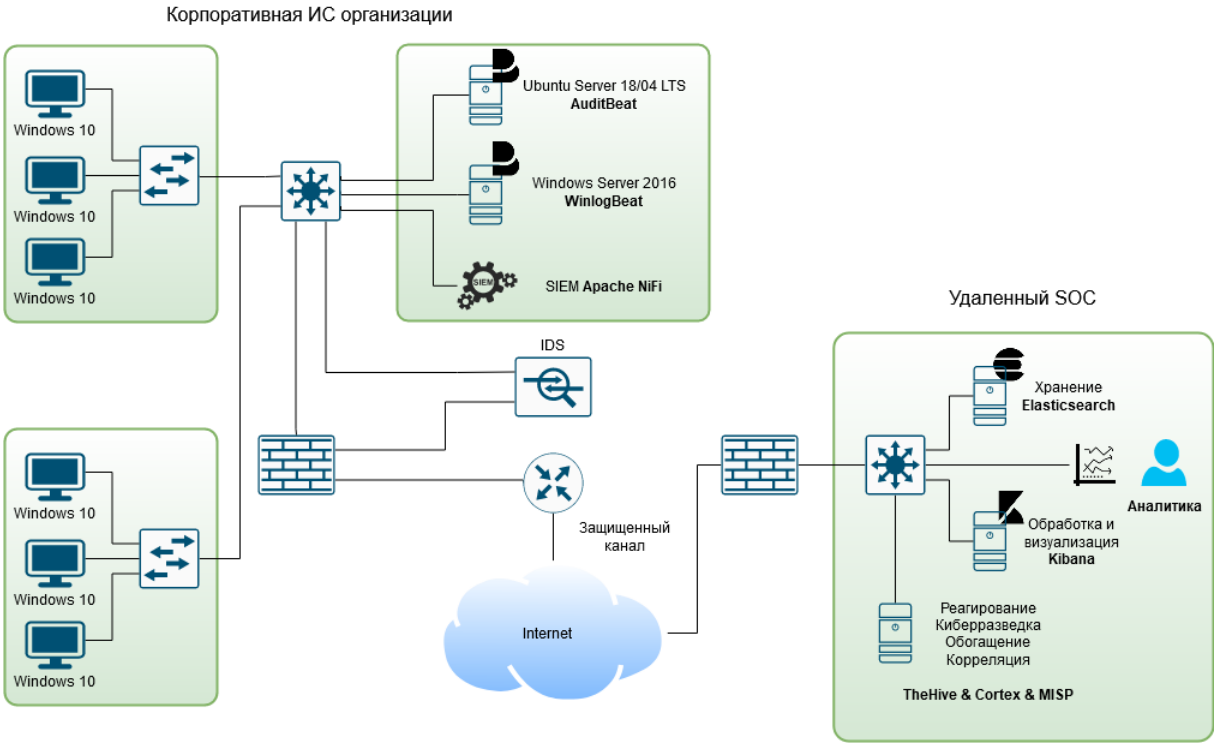

Рисунок 2 – Фрагмент топологии КИС организации
Figure 2 – Fragment of corporate information system topology

Существующий центр мониторинга и реагирования на инциденты ИБ (SOC) организации основан на ELK-стеке (Elasticsearch, Beats, Logstash, Kibana) [14].

Процесс мониторинга разбит на 6 шагов.

1. Источники. Источником событий выступают AuditBeat и WinlogBeat [15-17] на серверах Ubuntu 18.04 LTS и Server Windows 2015 в КИС организации.
2. Сбор. Данные собираются в SIEM-системе Apache NiFi и отправляются в удалённый SOC по защищённому каналу.
3. Хранение происходит в Elasticsearch.
4. Данные обрабатываются и визуализируются с помощью Kibana.
5. Полученная информация анализируется экспертами.

Проблемой является оперативная аналитика на стороне SOC, так как с источников событий КИС организации приходит слишком большое количество событий, степень важности которых неизвестна. Процесс киберразведки на основе СУДК в действующем SOC позволит снизить нагрузку на экспертов.

В процессе киберразведки каждая СУДК может выступать в роли потребителя или в роли провайдера данных. Для организации системы управления данными киберразведки за основу была взята платформа Malware Information Sharing Platform (MISP) [18]. Предлагаемая структурная организация системы управления данными киберразведки включает три компонента (Рисунок 3):

– IRP-система TheHive, для получения уведомлений и реагирования;

– платформа киберразведки MISP, для корреляции событий и распространения информации о киберугрозах;

– платформа автоматизированного анализа Cortex, для обогащения событий и собственно анализа.

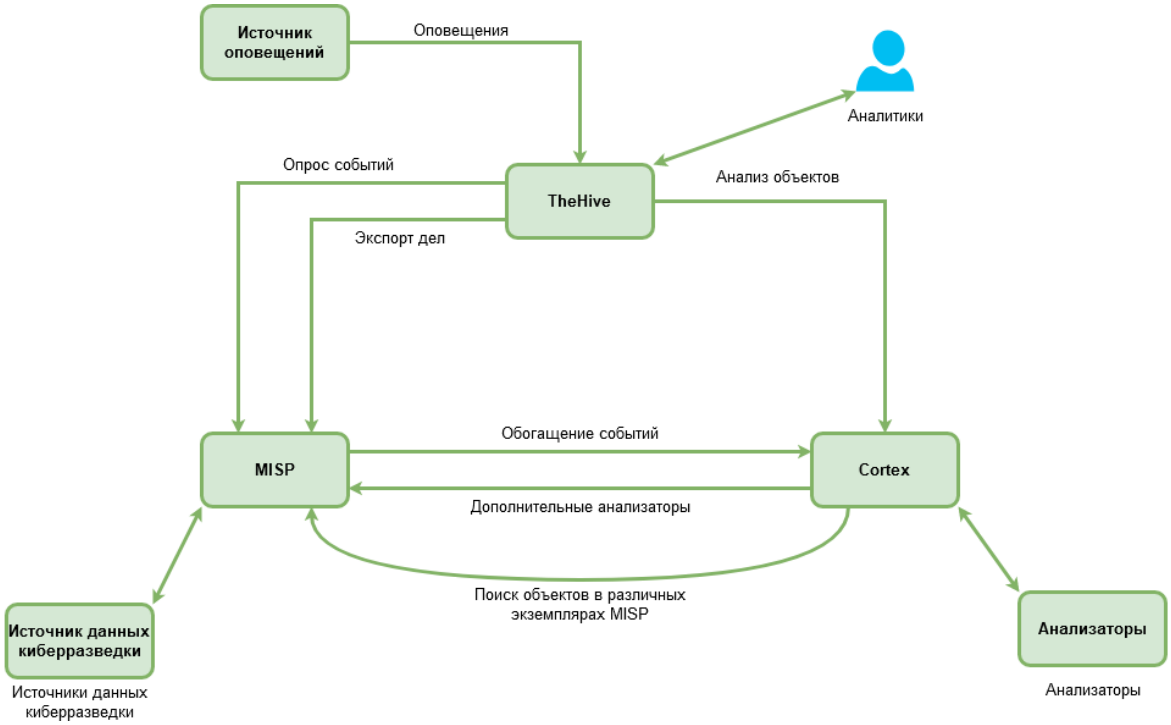

Рисунок 3 – Структурная схема предлагаемого СУДК
Figure 3 – Structural diagram of the proposed cyber threat intelligence platform

Фрагмент функциональной модели процесса кибербразведки представлен на Рисунке 4.

Принцип работы СУДК следующий. Уведомления приходят из источника в TheHive, объединяются и формируются в дело (case) с набором атрибутов (индикаторов). Далее дело экспортируются в MISP. В платформе MISP оно появляется в виде события с тем же набором атрибутов. Для него сразу же отображается количество совпадений с источниками данных (feeds hit) и количество корреляций с уже существующими событиями (correlation). Далее его можно обогатить (enrich) с помощью Cortex. Выбирается нужный анализатор, например, VirusTotal, затем атрибуты проходят через платформу Cortex, а новые данные (результаты антивирусной проверки) сразу добавляются в качестве атрибутов. Это обротанное событие с полной информацией можно опубликовать для других участников сообщества. Опубликованные события, помимо прочих платформ MISP, попадают и в TheHive, в котором можно осуществить расследование и реагирование, путём выдачи заданий (task) для выполнения разными специалистами.

Эти этапы могут быть автоматизированы с помощью PyMISP, TheHive4py, Cortex4py – библиотеками Python для доступа к соответствующим платформам через REST API. Помимо существующих анализаторов Cortex, новые анализаторы могут быть написаны на любом языке программирования, поддерживаемом ОС Linux, например, Python, Ruby, Perl и т. д.

Для расчёта необходимых для реальной нагрузки ресурсов сервера использован инструмент MISP-sizer [19]. На основе количества пользователей, количества атрибутов и доли корреляций MISP-sizer вычисляет необходимые значения оперативной памяти, объёма жёсткого диска, и количество процессоров. Ориентировочные требования к системе при 10 пользователях, 1 млн атрибутов и доле корреляций в 25% составляют: ОЗУ – 19 Гб, объем дисковой подсистемы – 1 Тб, 3 ядра CPU.

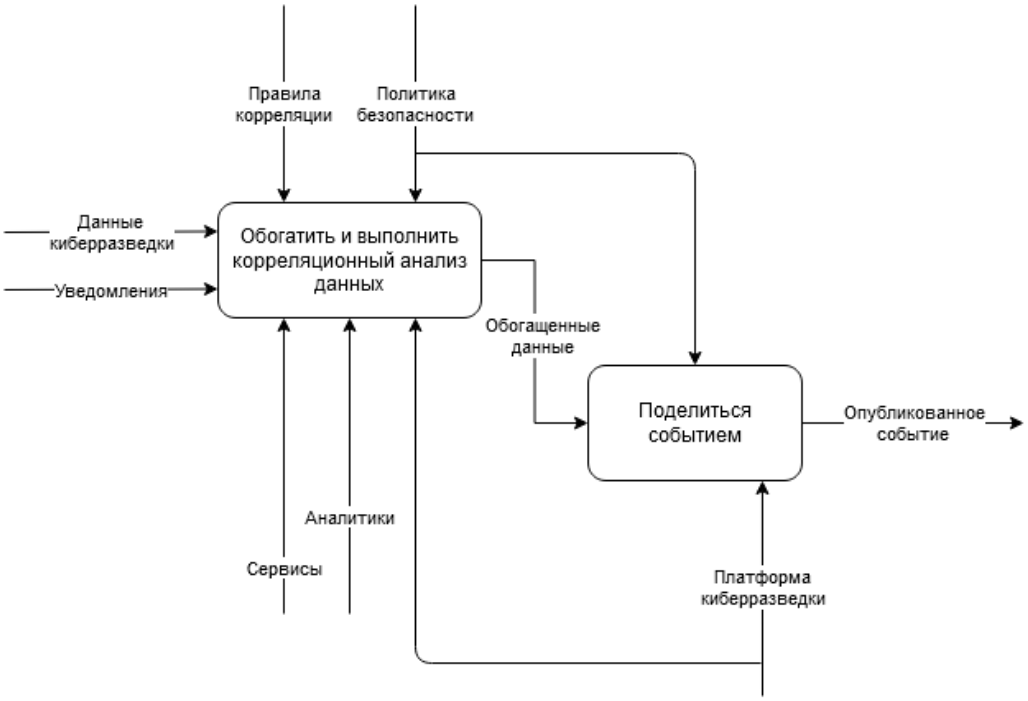

Рисунок 4 – Фрагмент функциональной модели процесса кибербразведки
Figure 4 – Fragment of the functional model of the cyber intelligence process

Установка платформ MISP, TheHive, Cortex может выполняться как на физические сервера, так и на виртуальные машины. В данном случае был выбран вариант с виртуальной машиной.

План развертывания СУДК включает следующие шаги:

- установка TheHive & Cortex;
- подключение TheHive к источнику событий и настройка шаблонов;
- установка MISP;
- интеграция MISP;
- подключение источников MISP;
- включение анализаторов Cortex.

Оценка эффективности применения СУДК в составе SOC

Для оценки эффективности и степени зрелости SOC используется методика SOMM (Security Operations Maturity Model) [20-21], основанной на CMMI и разработанной университетом Карнеги – Меллона [22-23]. Разделение процесса развития SOC на 5 стадий приведено в Таблице 4.

Таблица 4 – Уровни модели оценки зрелости SOC (SOMM)
Table 4 – SOC Maturity Assessment Model Levels (SOMM)

Уровень SOMM	Оценка SOC	Описание
Уровень 0	Недостаточный	Ключевые составляющие SOC отсутствуют

Уровень 1	Начальный	Ведется мониторинг, но нет документированных процессов. Реагирование по ситуации
Уровень 2	Базовый	Выполнение нормативных и бизнес-требований. Большинство процессов документированы, но пересматриваются по ситуации
Уровень 3	Надлежащий	Процессы хорошо документированы, регулярно пересматриваются с учетом текущих лучших практик
Уровень 4	Осмысленный	Эффективность SOC регулярно оценивается по метрикам производительности. Процессы выстраиваются для достижения KPI бизнеса
Уровень 5	Экстремальный	По всем направлениям SOC приняты программы развития. Процессы максимально конкретизированы и отточены. Поддержание этого уровня требует больше инвестиций, чем возможная отдача от них.

Методика использует принцип разделения показателей функционирования SOC на 5 аспектов: бизнес, люди, процессы, технологии и сервисы, в каждом из которых от 4 до 7 критериев. Эксперт отвечает на 10-20 вопросов по каждому критерию. По результатам ответов на них каждому критерию выставляется балл в диапазоне от 0 до 5. Общей оценкой аспекта является среднее арифметическое по критериям, входящим в этот аспект. Окончательная оценка SOC выставляется как среднее арифметическое по всем аспектам. Для более объективной картины привлечена группа из 4 экспертов:

Качество оценки эксперта определяется по формуле (1):

$$K_{эi} = 0,4K_{самi} + 0,6K_{взi}, \quad (1)$$

где $K_{эi}$ – качество оценки i-го эксперта,

$K_{самi}$ – коэффициент самооценки i-го эксперта,

$K_{взi}$ – коэффициент взаимооценки.

Коэффициент самооценки показывает, насколько, по мнению самого эксперта, он сам знаком с анализируемым объектом.

Коэффициент взаимооценки показывает оценку эксперта другими экспертами по профессиональной компетентности. Данный коэффициент находится по формуле (2):

$$K_{эi}^{H} = \frac{K_{эi}}{\sum_{j=1}^{m} K_{эi}}, \quad (2)$$

где $K_{эi}^{H}$ – нормированное значение качества оценки i-го эксперта,

$K_{эi}$ – качество оценки i-го эксперта,

$K_{эj}$ - качество оценки j-го эксперта.

Каждый эксперт проходит опрос, по его результатам выводится балл для каждого критерия. Элементы общего вектора критериев – средневзвешенная оценка данного критерия каждым экспертом (под весом здесь понимается качество оценки эксперта). Балл по аспектам – средний балл по критериям. В Таблице 5 представлены общие баллы по критериям и аспектам.

Таблица 5 – Общие баллы до и после внедрения СУДК
Table 5 – Total scores before and after platform implementation

К	Эксперт		

	Качество оценки	До внедрения СУДК		После внедрения СУДК	
		Общий вектор оценок	По аспектам	Общий вектор оценок	По аспектам
Бизнес	Бизнес-факторы	1,702	1,72	1,702	1,72
	Клиенты	1,421		1,421	
	Уставные документы	1,280		1,280	
	Руководство	1,883		1,883	
	Приватность	1,842		1,842	
Люди	Работники	2,191	1,54	2,191	1,54
	Роли и иерархия	1,010		1,010	
	Управление персоналом	1,500		1,500	
	Менеджмент знаний	0,568		0,568	
	Тренинги и обучение	2,430		2,430	
Процессы	Управление SOC	1,468	1,62	2,531	2,53
	Деятельность и аппаратура	2,451		2,451	
	Отчётность	0,999		2,316	
	Управление прецедентами	1,551		2,810	
Технологии	Инструменты SIEM	2,212	1,34	3,098	2,60
	Инструменты IDS/IPS	0,174		3,025	
	Инструменты анализа безопасности	2,332		2,332	
	Автоматизация	0,645		1,954	
Сервисы	Мониторинг безопасности	2,161	1,19	2,162	2,11
	Управления инцидентами безопасности	0,864		0,864	
	Анализ и экспертиза безопасности	1,620		1,620	
	Киберразведка	0		2,904	
	Поиск угроз	0		2,789	
	Управление уязвимостями	1,324		2,070	
	Управление логами	2,392		2,392	
	Уровень оценки	До	1,48	После	2,10

По итогам оценки уровень SOMM составляет 1,48 балла, что соответствует начальному уровню зрелости SOC. После внедрения оценка SOMM составила 2,10 что соответствует базовому уровню SOC (Рисунок 5).

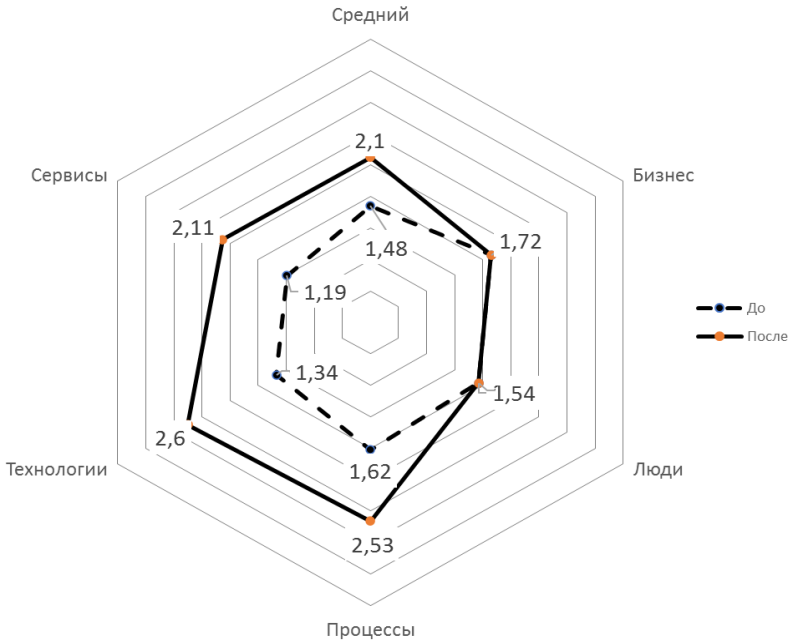

Рисунок 5 – Оценка зрелости SOC
Figure 5 – SOC maturity assessment

Наибольший прирост наблюдается в разделах «Технологии» и «Сервисы», в результате существенного повышения оценок по следующим критериям: «Кибербразведка», «Поиск угроз», «Управление прецедентами», «Инструменты IDS/IPS», «Мониторинг безопасности», «Управление уязвимостями». По результатам оценивания можно сделать вывод о повышении уровня эффективности SOC на 0,62 пункта или на 41,7% после развёртывания системы управления данными кибербразведки.

Заключение

Рассмотрены вопросы повышения эффективности центра мониторинга и реагирования на инциденты информационной безопасности за счет развертывания программной платформы управления данными кибербразведки. Применение платформы направлено на снижение нагрузки на специалистов, занимающихся мониторингом состояния информационной системы, в условиях возрастающего потока событий информационной безопасности.

В работе проанализированы подходы к реализации процесса и инструментов кибербразведки в составе SOC. Анализ рынка платформ кибербразведки показал, что наиболее распространенным решением с открытым исходным кодом является программное обеспечение MISP.

В процессе разработки структурной и функциональной моделей работы СУДК в составе SOC выделены основные задачи системы управления данными кибербразведки, а процесс реагирования разделён на отдельные шаги.

Разработан план и выполнено развертывание СУДК, включая подготовительную работу, установку, настройку и тестирование. План развертывания СУДК и результаты интеграционного тестирования платформы в реальном программном окружении позволят в дальнейшем автоматизировать перенос и масштабирование системы.

Применение методики SOMM до и после внедрения СУДК на основе ПО MISP показала, что эффективность функционирования центра мониторинга и реагирования на

инциденты ИБ выросла на 41,7%, а уровень зрелости SOC повысился с «начального» до «базового».

Благодарности

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) № 1/2020.

ЛИТЕРАТУРА

1. Петренко С.А., Петренко А.С. Концепция раннего распознавания предупреждения компьютерного нападения. *Материалы Всероссийской научно-практической конференции «Информационные системы и технологии в моделировании и управлении»*. 2016:82-86.
2. Какие задачи должен решать корпоративный центр мониторинга и реагирования на инциденты информационной безопасности (SOC). . URL: https://rvision.pro/en/blog-posts/kakie-zadachi-dolzhen-reshat-korporativnyj-tsentr-monitoringa-i-reagirovaniya-na-intsidenty-informatsionnoj-bezopasnosti-soc/ (дата обращения: 17.12.2020).
3. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности. *Стратегическая стабильность*. 2018;1:64-67.
4. Мишурин А.О. Перспективные направления развития технологий для центров мониторинга и реагирования на инциденты информационной безопасности. *Сборник II Межвузовской научно-практической конференции «Информационная безопасность: современная теория и практика».* 2019:89-93.
5. Бармин С.В. и др. Автоматизация и визуализация деятельности центров мониторинга и реагирования на ИБ-инциденты. *Защита информации. Инсайд.* 2019;4:44-51.
6. Королёв В.И. Процессная модель мониторинга и реагирования на инциденты информационной безопасности. *Сборник статей по материалам III Международной научно-практической конференции «Информационная безопасность: вчера, сегодня, завтра»*. 2020:18-25.
7. Ададуров С.Е. и др. Реагирование на инциденты информационной безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики. *Двойные технологии*. 2018;2:76-81.
8. ГОСТ Р ИСО/МЭК 27001 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
9. Security Threat Intelligence Products and Services Reviews and Ratings. . URL: https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendors (дата обращения: 17.12.2020).
10. Threat Intelligence: What is it, How Can it Protect You from Today's Advanced Cyber-Attacks?. URL: https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf (дата обращения: 17.12.2020).
11. Туманов Д., Абрамов Е. Разработка системы анализа и верификации индикаторов компрометации (IoC). *Безопасность информации и компьютерных сетей (SIN 2019).* 2019:54-57.

12. Мельников И. Краткий анализ рынка Threat Intelligence Platforms. . URL: https://www.volgablob.ru/blog/?p=1842 (дата обращения: 17.12.2020).
13. Ефремов Р. Автоматизация процессов киберразведки на основе решений класса Threat Intelligence Platform (TIP). URL: https://www.anti-malware.ru/practice/methods/threat-intelligence-platform (дата обращения: 17.12.2020).
14. Ahmed F. et al. Centralized Log Management Using Elasticsearch, Logstash and Kibana. *2020 International Conference on Information Science and Communication Technology (ICISCT). IEEE*. 2020:1-7.
15. Malhotra A., Rawat L., Kumar L. MINI SECURITY OPERATIONS CENTER USING ELK. *International Research Journal of Modernization in Engineering Technology and Science*. 2020;02(11):461-466.
16. Srivastava A., Miller D. *Elasticsearch 7 Quick Start Guide: Get up and running with the distributed search and analytics capabilities of Elasticsearch*. Packt Publishing Ltd, 2019.
17. Фетисов А.А. и др. Сбор и обработка лог файлов в макете комплекса поведенческого анализа трафика сети. *Состояние и перспективы развития современной науки по направлению «Информационная безопасность»*. 2020:54-58.
18. Wagner C. et al. Misp: The design and implementation of a collaborative threat intelligence sharing platform. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. 2016:49-56.
19. MISP Hardware Sizer (calculator). URL: https://www.misp-project.org/MISP-sizer/ (дата обращения: 17.12.2020).
20. White G.B. The community cyber security maturity model. *2011 IEEE international conference on technologies for homeland security (HST). IEEE*. 2011:173-178.
21. Caralli R.A., Allen J.H., White D.W. *CERT Resilience Management Model-CERT-RMM: A Maturity Model for Managing Operational Resilience*. Addison-Wesley Educational Publishers Inc. 2016.
22. Team C.P. CMMI for Development, version 1.2. 2006.
23. Денис М. Ахен, Арон Клауз, Ричард Тернер *CMMI: Комплексный подход к совершенствованию процессов. Практическое введение в модель*. М: «МФК». 2005.

REFERENCES

1. Petrenko S.A., Petrenko A.S. Concept of early detection and prevention of computer attack. *Materials of the All-Russian Scientific and Practical Conference «Information Systems and Technologies in Modeling and Control»*. 2016:82-86.
2. What tasks should the corporate center for monitoring and responding to information security incidents (SOC) solve. Available at: https://rvision.pro/en/blog-posts/kakie-zadachi-dolzhen-reshat-korporativnyj-tsentr-monitoringa-i-reagirovaniya-na-intsidenty-informatsionnoj-bezopasnosti-soc/ (accessed 17.12.2020).
3. Aksenenko Yu.I., Vasilenko V.V., Sidak A.A. Methodologic approach for constructing complex systems of monitoring and response on information security incidents. *Strategicheskaja stabil'nost'*. 2018;1:64-67.
4. Mishurin A.O. Perspektivnye napravlenija razvitija tehnologij dlja centrov monitoringa i reagirovanija na incidenty informacionnoj bezopasnosti. *Sbornik II Mezhvuzovskoj*

nauchno-prakticheskoj konferencii "Informacionnaja bezopasnost': sovremennaja teorija i praktika". 2019:89-93.
5. Barmin S.V. et al. Automation and visualization of the processes pursued by security operation centers and response to is incidents. *Zaŝita informacii. Inside*. 2019;4:44-51.
6. Korolev V.I. Process model for monitoring and response information security incidents. *Sbornik statej po materialam III Mezhdunarodnoj nauchno-prakticheskoj konferencii "Informacionnaja bezopasnost': vchera, segodnja, zavtra"*. 2020:18-25.
7. Adadurov S.E. el al. Response to information security incidents in microprocessor systems of railway automatics and telemehanics. *Dvojnye tehnologii*. 2018;2:76-81.
8. GOST R ISO / IEC 27001 Information technology (IT). Security methods and means. Information security management systems. Requirements.
9. Security Threat Intelligence Products and Services Reviews and Ratings. Available at: https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendors (accessed 17.12.2020).
10. Threat Intelligence: What is it, How Can it Protect You from Today's Advanced Cyber-Attacks? Available at: https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf (accessed 17.12.2020).
11. Tumanov D., Abramov E. Razrabotka sistemy analiza i verifikacii indikatorov kompрometacii (IoC). *The XII International Conference on Security of Information and Networks.* 2019:54-57.
12. Melnikov I. Threat Intelligence Platforms Market Brief. Available at: https://www.volgablob.ru/blog/?p=1842 (accessed 17.12.2020).
13. Efremov R. Automation of cyber intelligence processes based on Threat Intelligence Platform (TIP) solutions. Available at: https://www.anti-malware.ru/practice/methods/threat-intelligence-platform (accessed 17.12.2020).
14. Ahmed F. et al. Centralized Log Management Using Elasticsearch, Logstash and Kibana. *2020 International Conference on Information Science and Communication Technology (ICISCT). IEEE*. 2020:1-7.
15. Malhotra A., Rawat L., Kumar L. MINI SECURITY OPERATIONS CENTER USING ELK. *International Research Journal of Modernization in Engineering Technology and Science*. 2020;02(11):461-466.
16. Srivastava A., Miller D. *Elasticsearch 7 Quick Start Guide: Get up and running with the distributed search and analytics capabilities of Elasticsearch*. Packt Publishing Ltd, 2019.
17. Fetisov A.A. et al. Sbor i obrabotka log fajlov v makete kompleksa povedencheskogo analiza trafika seti. *Sostojanie i perspektivy razvitija sovremennoj nauki po napravleniju «Informacionnaja bezopasnost»*. 2020:54-58.
18. Wagner C. et al. Misp: The design and implementation of a collaborative threat intelligence sharing platform. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. 2016:49-56.
19. MISP Hardware Sizer (calculator). Available at: https://www.misp-project.org/MISP-sizer/ (accessed 17.12.2020).
20. White G.B. The community cyber security maturity model. *2011 IEEE international conference on technologies for homeland security (HST). IEEE*. 2011:173-178.
21. Caralli R.A., Allen J.H., White D.W. *CERT Resilience Management Model-CERT-RMM: A Maturity Model for Managing Operational Resilience*. Addison-Wesley Educational Publishers Inc. 2016.

22. Team C.P. CMMI for Development, version 1.2. 2006.
23. Denis M. Aachen, Aaron Clause, Richard Turner *CMMI: Integrated Approach to Process Improvement. Practical Introduction to the Model*. M: «MFK». 2005.

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Вульфин Алексей Михайлович, к.т.н., доцент, кафедра вычислительной техники и защиты информации, ФГБОУ ВО "Уфимский государственный авиационный технический университет", Уфа, Российская Федерация.
e-mail: vufin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Aleksey M. Vulfin, PhD Student, Department of Computing and Information Security, Federal State Budgetary Institution of Higher Education "Ufa State Aviation Technical University", Ufa, Russian Federation