



RUSIEM

Всё под контролем

***SIEM-система
как один из основных элементов
информационной безопасности
организации***

***Иван Кандалов,
менеджер по работе с ключевыми заказчиками¹***

Что такое SIEM

Компания

Занимается созданием решений в области мониторинга и управления событиями информационной безопасности и ИТ-инфраструктуры на основе анализа данных в реальном времени

Полностью
российская разработка
(с 2014 года)

Продукт включен в Единый
реестр отечественного ПО,
имеет сертификаты ФСТЭК
России (4 УД), ОАЦ (Беларусь)

Резидент
Сколково

>570 Партнеров в России и
странах СНГ

Продукт

Программный комплекс обеспечения информационной безопасности, позволяющий собирать и анализировать информацию о событиях ИБ, получаемую из разнородных источников

Работа RuSIEM позволяет увидеть максимально полную картину активности сетевой инфраструктуры и событий информационной безопасности

Схема работы SIEM



Рабочие станции



Firewall



Роутеры



Сетевые
коммуникаторы



Серверы



Мейнфреймы



Системы обнаружения
и предотвращения
вторжений

SIEM



Предупреждения



Дашборды



Журнал событий



Отчеты



Мониторинг

Какие задачи решает SIEM



Оперативное обнаружение, реагирование и контроль обработки инцидентов



Оперативный контроль состояния инфраструктуры компании



Создание единого центра мониторинга



Определение прав, обязанностей и разграничение зон ответственности персонала компании (ИТ- и ИБ-служб)



Соответствие требованиям регуляторов
(Федеральные законы № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказы ФСТЭК России № 21, 17 и 31, СТО БР ИББС и РС БР ИББС-2.5-2014, международного стандарта PCI DSS, ISO 27001)

Источники событий для SIEM

- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы
- Контроллер домена
- Межсетевые экраны
- IDS/IPS
- DNS logs
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения

Пример использования SIEM



- Access Control, Authentication
- DLP-системы
- IDS/IPS-системы
- Антивирусные приложения

- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Сетевое активное оборудование
- Сканеры уязвимостей

- Система инвентаризации и asset-management (а у некоторых СИЕМ есть даже свой внутренний функционал работы с активами)
- Система веб-фильтрации

Линейка продуктов



RvSIEM (free)

– классическое решение класса LM



RuSIEM

– коммерческая версия класса SIEM



RuSIEM Analytics

– модуль для анализа событий, основанный на ML



RuSIEM IoC

– модуль индикаторов компрометации



RuSIEM Monitoring

– модуль мониторинга информационных систем, узлов, приложений

Лицензирование

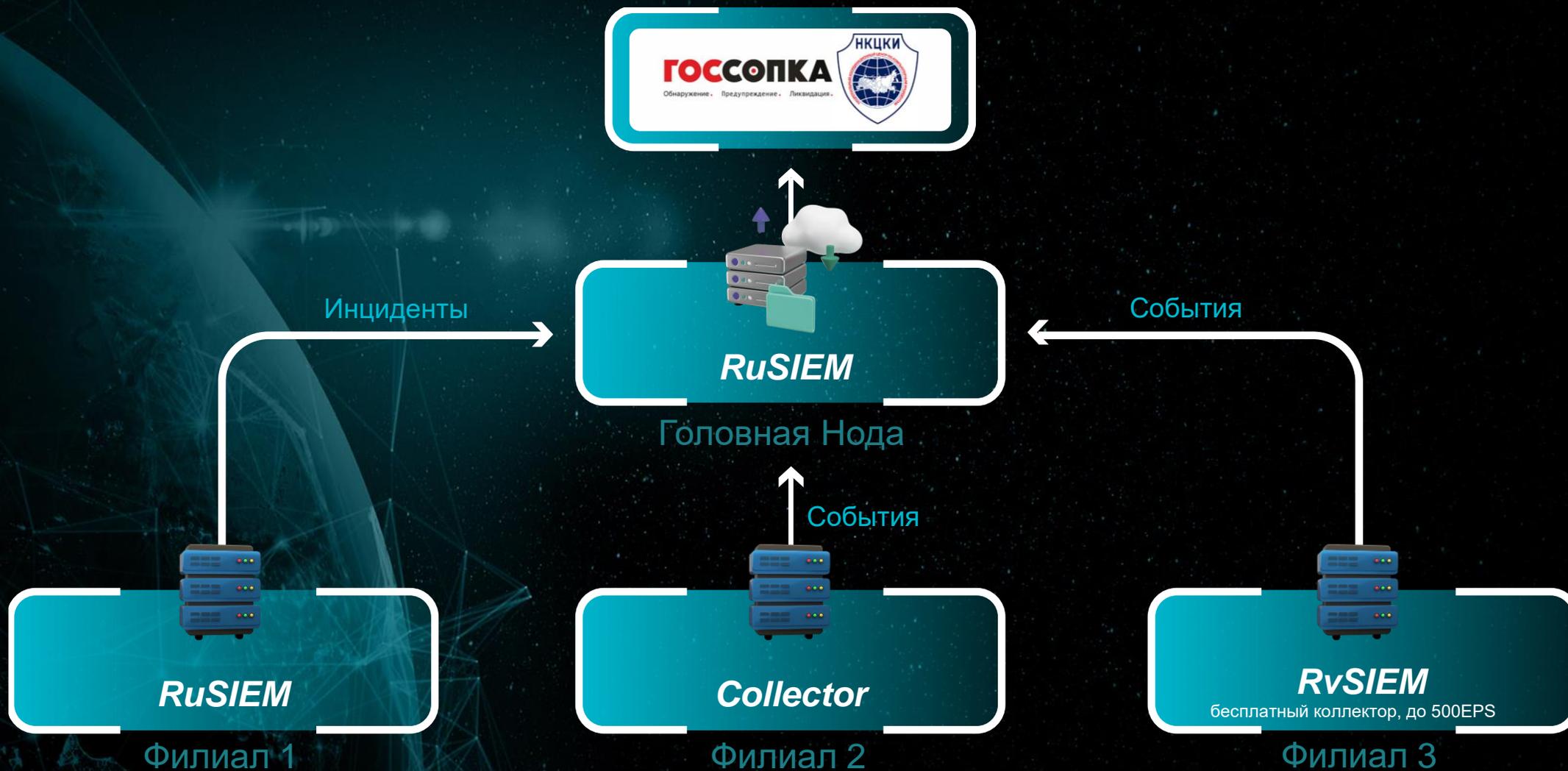
Кол-во событий в секунду
(Event per second)

- Проектные цены
- Модульные спецификации
- Бессрочные и срочные лицензии
- Разработка сложных парсеров
- Разработка правил корреляции
- **Безлимитная лицензия – новинка!**

2000 eps
3000 eps
4000 eps
5000 eps
7500 eps
10000 eps
12500 eps
15000 eps
20000 eps

...

Варианты развертывания системы



SOC на RuSIEM

SOC был развернут для ряда крупных заказчиков на SIEM-системе RuSIEM совместно с партнерами



Масштабирование горизонтальное, распределение нагрузки



- Производительность
- «Горячее» расширение без остановки сбора
- Поддержка слабых каналов между удаленными объектами
- Корреляция в центральном офисе без необходимости передачи всех событий «наверх»
- Распределенный поиск по событиям без необходимости «единого хранилища»

Почему RuSIEM?

Отечественная
разработка,
техническая
поддержка на
русском языке

Решение
подойдет
компаниям
любого
масштаба

Возможность
горизонтального и
вертикального
масштабирования

Широкая
партнерская сеть

Оперативное
реагирование
на запросы
заказчиков по
добавлению
нового
функционала

Высокая
точность
выявления
событий «из
коробки» 97%*

Более 400
правил
корреляции
для анализа
событий

Отсутствуют
ограничения
по размеру
архивного
хранилища

Референсы

АКСОН



Благодарственное письмо

Уважаемый Роман Александрович!

Настоящим компания «АКСОН» выражает благодарность ООО «РУСИЕМ» за партнерское участие в реализации на инцидент информационной безопасности, ликвидацию его последствий и содействие в дальнейшем укреплении периметра защиты компании на базе SIEM-системы собственной разработки компании.

АКСОН — крупнейшая российская динамично развивающаяся сеть магазинов для дома и ремонта с омниканальной системой продаж и высоким уровнем логистического сервиса. Компания представлена в 3 федеральных округах, 10 областях и 14 городах. АКСОН занимает 2 место среди отечественных ритейлеров по количеству сервисов крупнейших розничных и оптово-розничных операторов сегмента Hard/Soft DIY. Значительная доля бизнеса компании приходится на онлайн-каналы; так, ежемесячный трафик интернет-магазина составляет 1 млн посетителей. В этой связи непрерывность практически любых IT-процессов имеет ключевое значение для бизнеса компании.

В марте 2021 года компания подверглась мощнейшей кибератаке. В России на данный момент практически отсутствуют требования к обеспечению требований информационной безопасности информационных систем на стадии их разработки. Очень немногие IT-компании уделяют киберустойчивости своих решений необходимое внимание. В результате даже те организации, где разработаны и внедрены политики и соблюдаются стандарты информационной безопасности, сталкиваются с рисками реализации различных угроз. В нашем случае это была атака преступной группы, которая использовала уязвимости иностранного ПО, получила доступ к системам управления ридом сервисов, перекватила иностранного ПО, получила доступ к базам данных и потребовала уплаты выкупа в течение двух суток. В случае отказа злоумышленники угрожали заблокировать доступ ко всем управляющим серверам, что было бы равносильно полной остановке всех бизнес-процессов.

Необходимо было принять решение: выплатить выкуп и не обращаться за помощью либо найти компанию, которая в оперативном режиме и профессионально обнаружит угрозы, устранит их, заблокирует злоумышленникам доступ к инфраструктуре и установит систему для предотвращения подобных угроз в дальнейшем, а также обратиться за помощью в БСТМ МВД России.

Среди существующих на рынке решений выбор был сделан в пользу решения от ООО «РУСИЕМ». Учитывая территориальную распределенность нашей компании и количество оборудования в каждой локации, ни один другой продукт не решал нашу задачу. Уже в день обращения специалисты компании подключились к исследованию. От обращения до блокировки угрозы и разветвления полноценной SIEM-системы прошло два часа, при этом мы не наблюдали каких-либо сложностей с интеграцией. В течение суток были выявлены точки проникновения и зарезанные узлы, ограничено распространение ВТО, использован симметрированный сегмент сети и выстроен периметр защиты. Собранные данные были переданы сотрудникам органов.

На сегодняшний день система позволила компании «АКСОН» решить следующие ключевые с точки зрения обеспечения непрерывности бизнеса и киберустойчивости его процессов задачи:

- реализация качественного мониторинга происходящих в инфраструктуре ООО «АКСОН» событий безопасности;
- создание единой точки входа;
- настройка контроля и защиты периметра;
- разработка и внедрение усиленной ИБ-политики.

Решение «РУСИЕМ» помогает нам в реальном времени оценивать защищенность информационных систем и минимизировать риски информационной безопасности. Так, с момента развертывания системы было предотвращено несколько возможных инцидентов.



В ООО «РУСИЕМ»

Иск. № 4/4 от 14.12.2021г.

Благодарственное письмо

ООО СК «УРАЛСИБ СТРАХОВАНИЕ» (ОГРН 1027739608005, ИНН 7606001534, КПП 772801001)

(далее – Компания) в лице Заместителя генерального директора по ИТ и операционной деятельности Буто Владислава Андреевича, выражает благодарность ООО «РУСИЕМ» за разработку и внедрение SIEM-системы RuSIEM в Компанию, позволившей повысить эффективность выявления потенциальных инцидентов информационной безопасности и обеспечить своевременное реагирование на них. Предложенное компанией ООО «РУСИЕМ» решение позволяет обеспечить контроль соблюдения политики информационной безопасности, решая следующие задачи:

- контроль большого количества событий, поступающих с внутренних систем критических сегментов заказчика и из пользовательских сегментов;
- выявление новых угроз путем корреляции данных из различных источников, включая АРМ, серверную подсистему, сетевые компоненты;
- проверка гипотез при появлении новых уязвимостей и угроз;
- централизованное хранение данных и быстрый поиск по событиям информационной безопасности (далее – ИБ);
- поведенческий анализ на базе собранной статистики и выявление случаев отклонения от статистической модели;
- получение уведомлений о выявленных подозрительных событиях в журнал.

Сотрудники ООО «РУСИЕМ» помогли установить систему RuSIEM, подключить источники, написать и доработать ряд пароворов. В результате наша Компания получила инструмент, значительно ускоряющий процесс обработки инцидентов ИБ и обеспечивающий получение требуемой информации о событиях ИБ в консолидированном виде в едином удобном интерфейсе. Благодаря использованию хранящейся в системе дополнительной информации, расследовать инциденты стало намного проще.

Мы рассчитываем на то, что с операционной и экономической точки зрения расходы на внедрение системы RuSIEM окупат себя в ближайшее время, т.к. автоматизация обработки инцидентов ИБ позволяет избежать затрат на персонал, необходимый для контроля всех средств защиты информации в ручном режиме. Также хотим отметить, что раннее выявление потенциальных угроз минимизирует возможные экономические потери от потенциальной утечки данных клиентов или хищения денежных средств.

Выражаем искреннюю благодарность коллективу ООО «РУСИЕМ» за профессионализм, оперативность и ответственный подход к решению задач ООО СК «УРАЛСИБ СТРАХОВАНИЕ» полностью удовлетворены качеством работы и уровнем компетенции сотрудников ООО «РУСИЕМ» и рекомендуем компанию как надежного партнера.

Заместитель генерального директора по ИТ и операционной деятельности

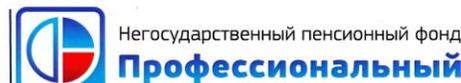


В.А. Буто

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
СТРАХОВАЯ КОМПАНИЯ «УРАЛСИБ СТРАХОВАНИЕ»
ИН 7606001534, ОГРН 1027739608005
Тел: (495) 781-71-53, факс: (495) 781-00-64
e-mail: info@uralsib.ru

Адрес: ул. Профсоюзная, д. 65, корпус 1, эт. 15, пом. 1517, Москва, Россия 117342
ОГРН 1027739608005, ИНН 7606001534, КПП 772801001

ПРОФЕССИОНАЛЬНЫЙ
негосударственный пенсионный фонд



Адрес: 119000, г. Москва, ул. Чкаловская, д. 11, эт. 5
ИНН/КПП 7701399098/770101001
р/с: 40701810895000001960
С/ч/с: 30101810200000000023
БИК: 044525262

иск. № ИСК202206011
от 01.06.2022

Благодарственное письмо

Настоящим Негосударственный пенсионный фонд «Профессиональный» (Акционерное общество) выражает искреннюю благодарность ООО «РУСИЕМ» за помощь во внедрении и технической поддержке системы обнаружения вредоносной активности, мониторинга и управления событиями информационной безопасности на базе SIEM-системы RuSIEM.

SIEM-система RuSIEM позволила НПФ «Профессиональный» (АО) обеспечить соответствие требованиям Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных требований для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Отдельно хотелось бы отметить профессионализм, оперативность и ответственный подход сотрудников ООО «РУСИЕМ» по обеспечению информационной безопасности.

Рекомендуем участникам финансового сектора рынка обратить внимание на SIEM-систему RuSIEM при решении задач, связанных с выполнениями требований ГОСТ 57580.1-2017.

НПФ «Профессиональный» (АО) заинтересован в дальнейшем сотрудничестве с компанией ООО «РУСИЕМ», развитии и совместной реализации новых масштабных проектов.

Президент



Ю. А. Зверев



БИЗКОММ

Юридический адрес: Хлебобулочный проезд, д. 7, стр. 9,
эт. 3, пом. 3, кон. 25, кв. 14, Москва, Россия, 115230
Почтовый адрес: 89 85, Москва, Россия, 115334
ОГРН 1117746926993 / ИНН 7714856880 / КТД 772401001
Телефон: +7 (495) 900-18-65
www.bizkomm.ru

18.04.2022 № ИСК-БК-2204181-3
На № _____ от _____

О направлении благодарственного письма

Уважаемый Роман Александрович!

Благодарю Вас за профессиональный подход, своевременную помощь и техническую поддержку, оказанную специалистами ООО «РУСИЕМ» в ходе реализации мероприятий по созданию информационной системы мониторинга и управления событиями информационной безопасности на базе программного обеспечения «RuSIEM», используемой в ООО «БизКомм» для обеспечения лицензированной деятельности по мониторингу событий информационной безопасности.

С уважением,
Заместитель
генерального директора

А.В. Пестунов

ООО «РУСИЕМ»
Генеральному директору
Р.А. Вороницу

Референсы



Алкогольная
Сибирская
группа



Центр международных расчетов



ИНСТИТУТ
АЭРОНАВИГАЦИИ

АКЦИОНЕРНО-ОБЩЕСТВО
«ГОМЕЛЬСКИЙ ХИМИЧЕСКИЙ ЗАВОД»
ул. Химиковская, 5, 246026, г. Гомель
УНП 40009095, ОКПО 000217143990
Факс: +375 232 23 12 42, тел.: +375 232 23 12 90
E-mail: abonem@belfertzavod.by
http://belfert.by

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«ГОМЕЛЬСКИЙ ХИМИЧЕСКИЙ ЗАВОД»
ул. Химиковская, 5, 246026, г. Гомель
УНП 40009095, ОКПО 000217143990
Факс: +375 232 23 12 42, тел.: +375 232 23 12 90
E-mail: abonem@belfertzavod.by
http://belfert.by

20.07.2023 № 33/12214
На № _____ от _____

Генеральному директору
ООО «РУСИЕМ»
Вороницу Роману Александровичу

Благодарственное письмо

Открытое акционерное общество «Гомельский химический завод» является одним из ведущих предприятий нефтехимической отрасли Беларуси и крупнейшим в стране, выпускающим фосфорсодержащие минеральные удобрения, основными задачами которого являются обеспечение потребностей сельхозпроизводителей Республики Беларусь, а также частичное удовлетворение зарубежных рынков, в минеральных удобрениях, средствах защиты растений, прочей химической продукции (сульфит натрия, фтористый алюминий, криолит и др.), повышение их качества и конкурентоспособности на отечественном и зарубежном рынках, создание условий для успешного экономического развития предприятий.

Для реализации основных задач наше предприятие постоянно совершенствует свои технологии, в том числе развивая ИТ-инфраструктуру, важной частью которой являются системы информационной безопасности. В рамках развития информационной безопасности был проведен ряд пилотных проектов многофункциональных SIEM-систем.

Продукт компании RuSIEM стал одним из лидеров нашего выбора после проведения пилота системы. В ходе проекта была проведена подробная презентация, внедрение и тестирование SIEM-системы RuSIEM. Мы были полностью удовлетворены результатом работы системы. Выражаем благодарность технической команде компании RuSIEM за оперативную поддержку решения и компании ИРСИЕМ ГРУПП за успешное проведение пилота!

Первый заместитель директора -
главный инженер
Иванчук А.С. (0232) 23-12-16

В.В.Осипенко



Генеральному директору ООО «РУСИЕМ»
Вороницу Роману Александровичу

Благодарственное письмо

«Алкогольная Сибирская Группа» (АСГ) является одним из крупнейших производителей алкоголя. По итогам 2021 года объем производства продукции под брендами компании составил 8,3 млн. дал.

Сложность производственных процессов, их бесперебойность, автоматизация и цифровизация производства предполагают постоянный контроль и усиление информационной безопасности, чтобы не допустить сбоя на всех этапах.

Для решения этой задачи АСГ выбрала продукт компании RuSIEM. SIEM-система российского производства RuSIEM полностью соответствует требованиям АСГ по контролю и анализе сетевой активности (благодаря дополнительному модулю RuSIEM Analytics), обнаружению и реагированию на инциденты.

Благодарим ООО «РУСИЕМ» за профессиональную работу, качественную поддержку при установке системы и своевременную обратную связь и по сей день. Можем рекомендовать данное решение для организаций с повышенными требованиями по сохранности данных и безопасности производственных процессов.

Иванов Виталий Александрович
Ведущий специалист по информационной безопасности
ООО «Алкогольная Сибирская Группа»



ЦМРБанк (общество с ограниченной ответственностью)
127015, Россия, Москва, г. Москва, ул. Пятовская, д. 18, стр. 7
Телефон: 8 (800) 210-09-22, 8 (495) 980-80-44
www.cmrbank.ru, e-mail: info@cmrbank.ru

Генеральному директору
ООО «РУСИЕМ»
Вороницу Р. А.

Универсальная лицензия Банка России № 1551 от 02 апреля 2018 года
ИНН 7750056670, ОГРН 1157700605759

30.01.2023 № 255

На _____ от _____

Благодарственное письмо Уважаемый Роман Александрович!

ООО «ЦМРБанк» выражает благодарность коллективу ООО «РУСИЕМ» за внедрение решения для мониторинга и реагирования на события информационной безопасности RuSIEM. Развертыванием системы банк подтвердил верность курса на обеспечение безопасности платежей, сохранение конфиденциальности расчетов, а также на стремление быть для действующих и новых клиентов доверенным партнером в финансах.

SIEM-система RuSIEM существенно усилила киберзащиту банка. На ее базе внедрена система управления событиями информационной безопасности, автоматизировано выявление внешних и внутренних угроз, а также выработаны стандартизированные процедуры реагирования на них.

Внедрение RuSIEM заняло несколько дней при поддержке инженеров компании-разработчика. В частности, они адаптировали для совместной работы с SIEM механику передачи событий для анализа, а также обучили ИБ-команду банка составлению правил корреляции, чтобы специалисты на стороне банка имели возможность гибко настраивать систему под специфичные сценарии.

Таким образом, SIEM-система RuSIEM не только обеспечила повышенный уровень информационной безопасности, но и стала важной составной частью риск-менеджмента ЦМРБанка.

Выражаем благодарность специалистам ООО «РУСИЕМ», а также надеемся на наиболее плодотворное сотрудничество.

Начальник отдела информационной безопасности _____ Итумрудский Н.В.



ФГУП «Госкорпорация по ОрВД»
Некоммерческое образовательное учреждение
дополнительного профессионального образования
«ИНСТИТУТ АЭРОНАВИГАЦИИ»
(Институт аэронавигации)



FSUE «State ATM Corporation»
Non-Commercial Education Institution
for supplementary professional training
«INSTITUTE OF AIR NAVIGATION»
(Institute of Air Navigation)

08.08.2023 № 377/1-01

на № _____

Генеральному директору
ООО «РУСИЕМ»
Вороницу Р.А.

Благодарственное письмо

Некоммерческое образовательное учреждение дополнительного профессионального образования «Институт аэронавигации» выражает благодарность ООО «РУСИЕМ» за поставку, внедрение и ввод в эксплуатацию решения для мониторинга и управления событиями информационной безопасности и ИТ-инфраструктуры RuSIEM.

Институт аэронавигации был создан в 2004 году. Образовательная организация специализируется на повышении квалификации и переподготовке специалистов Федерального государственного унитарного предприятия «Государственная корпорация по организации воздушного движения в Российской Федерации» по направлению организации воздушного движения, эксплуатации радиотехнического оборудования и авиационной электросвязи, а также проводит специализированное обучение авиационных специалистов на английском языке.

Максимальные издержки на российское государственное и частные предприятия в 2022 году стали поводом для дополнительных мер к обеспечению кибербезопасности Института аэронавигации. Одной из ключевых активностей в этом направлении стало развертывание решения для мониторинга и управления событиями информационной безопасности. Оно позволяет фиксировать попытки взлома организации, которые могут спровоцировать утечку данных и нарушение работы информационных систем, ведущие к финансовым и репутационным потерям.

В процессе выбора оптимального решения предпочтение было отдано программному обеспечению RuSIEM. Развертывание системы прошло на высоком профессиональном уровне. Оно позволило решить следующие задачи:

- оповещать специалистов по информационной безопасности об аномалиях внутри участков ИТ-инфраструктуры и вне ее и тем самым сигнализировать о возможных попытках взлома и о вероятных утечках данных;
- обеспечивать одинаковый для всех восьми филиалов Института аэронавигации уровень мониторинга;
- централизовать наблюдение и оповещение о событиях информационной безопасности для оперативного реагирования на них;
- предоставить специалистам по информационной безопасности новые возможности, такие как составление правил корреляции без навыков программирования для обеспечения чувствительности SIEM-системы к новым типам событий, а также автоматизация реагирования для локализации возможной инцидента.

Применение RuSIEM полностью отвечает курсу Института аэронавигации на усиление информационной безопасности и реализацию подхода к управлению ею как процессом.

Мы благодарим команду RuSIEM за гибкий и эффективный программный продукт и можем рекомендовать это решение для усиления информационной безопасности в организациях с повышенными требованиями к сохранности данных и надежности работы информационных систем.

Директор _____

М.М. Назаров



127015, Россия, Москва, ул. Большая Никитинская, д. 14, стр. 7
Тел.: +7 (495) 479-22-23
ИНН 7702056476, ОГРН 7715013051

Адрес: 127015, Россия, Москва, ул. Большая Никитинская, д. 14, стр. 7
Тел.: +7 (495) 479-22-23
E-mail: info@airnav.ru, www.airnav.ru

Telegram-каналы RuSIEM

[*https://t.me/rusiem*](https://t.me/rusiem)

последние новости, важные события



[*https://t.me/rusiemsupport*](https://t.me/rusiemsupport)

возможность быстро связаться с технической поддержкой



Спасибо за внимание!



www.rusiem.com



i.kandalov@rusiem.com



+7 (925) 411-48-30

