SOLAR

SOLAR JSOC

Памятка

О СООТВЕТСТВИИ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сервисы мониторинга и реагирования ГК «Солар»

W: RT-SOLAR.RU

ФЗ № 149 от 27.07.2006

Об информации, информационных технологиях и о защите информации

Государственные органы | Коммерческие организации | Некоммерческие организации

Ключевые требования к выполнению нормативного акта

01 Защита информации: организации обязаны обеспечивать защиту информации от несанкционированного доступа, уничтожения, модификации. Разработка и внедрение систем защиты информации, определение уровней доступа к данным

02 Обработка персональных данных: соблюдение норм по обработке персональных данных, включая согласие субъектов. Обязанность уведомлять субъекты о целях и методах обработки их данных

03 Информационная безопасность: создание условий для безопасного функционирования информационных систем. Проведение аудитов и оценки рисков в области информационной безопасности

04 Документирование процессов: ведение документации, касающейся обработки и защиты информации, разработка внутренних регламентов и инструкций

05 Обучение сотрудников: обучение и повышение квалификации работников в области информационной безопасности и защиты информации

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для выполнения общих требований по защите информации необходимо использовать решения ИБ, которые:

- Позволяют проводить аудит и мониторинг информации и действий сотрудников в системах, что помогает соблюсти требования по документированию процессов
- Собирают и анализируют данные из различных источников, таких как сетевое оборудование, серверы, приложения и базы данных, для выявления подозрительной активности
- Анализируют сетевую активность, выявляют аномалии

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Сервисы ГосСОПКА
- Мониторинг АСУ ТП и объектов КИИ
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)
- Управление процессами реагирования на киберинциденты (IRP)

Использование этих сервисов позволяет организациям не только отслеживать инциденты безопасности, но и запускать процессы быстрого реагирования в соответствии с законом о защите информации с целью уменьшения рисков от киберугроз

ФЗ № 152-ФЗ от 27.07.2006

О персональных данных

Государственные органы | Коммерческие организации | Некоммерческие организации | Индивидуальные предприниматели

Ключевые требования к выполнению нормативного акта

01 Получение согласия: обработка персональных данных допускается только с согласия субъекта персональных данных, за исключением случаев, предусмотренных законом (например, для выполнения обязательств по договору)

02 Цель обработки: персональные данные должны обрабатываться только в законных целях, которые должны быть четко определены и заранее известны субъекту

03 Минимизация данных: обработка должна ограничиваться минимально необходимым объемом персональных данных, соответствующим заявленной цели

04 Безопасность данных: организации обязаны принимать меры для защиты персональных данных от несанкционированного доступа, утечек и уничтожения, включая разработку и внедрение систем безопасности

05 Документированная политика: необходимо наличие документов, регулирующих обработку персональных данных, включая политику в области обработки, регламенты, инструкции и т. д.

06 Права субъектов персональных данных: субъекты имеют право на доступ к своим персональным данным, их исправление, удаление и ограничение их обработки. Организации обязаны информировать пользователей об их правах

07 Уведомление Роскомнадзора: в некоторых случаях организации обязаны уведомлять Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) о начале обработки персональных данных

08 Обучение сотрудников: обучение и повышение уровня осведомленности сотрудников о необходимости соблюдения норм защиты персональных данных

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для защиты персональных данных необходимо использовать решения, которые:

- Помогают организациям обнаруживать, анализировать и управлять инцидентами, связанными с обработкой персональных данных
- Позволяют проверять соответствие нормам безопасности и отслеживать действия пользователей в системах
- Автоматизируют процессы реагирования на инциденты, связанные с утечкой или компрометацией данных
- Идентифицируют уязвимости в системах и приложениях, которые могут повлиять на обработку персональных данных
- Обеспечивают предотвращение несанкционированного доступа к системам и данным

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)

Использование указанных сервисов помогает снижать риски, связанные с нарушениями в области безопасности, а также оперативно реагировать на инциденты, которые могут затронуть персональные данные

ФЗ № 98 от 29.07.2004

О коммерческой тайне

Коммерческие организации | Некоммерческие организации | Государственные и муниципальные учреждения

Ключевые требования к выполнению нормативного акта

01 Определение коммерческой тайны: организации должны четко определить, какая информация будет считаться коммерческой тайной, и должны иметь документы, подтверждающие это

02 Документирование и оформление: необходимо оформить доступ к коммерческой тайне и дать четкое определение данным, которые должны храниться в условиях конфиденциальности

03 Защита коммерческой тайны: разработать и реализовать меры по защите коммерческой тайны от разглашения и несанкционированного доступа. Это могут быть как технические меры (например, системы защиты данных), так и организационные (например, ограничение доступа)

04 Контроль и аудит: необходимо проводить периодический контроль за соблюдением режима коммерческой тайны и осуществлять аудит доступа к такой информации

05 Обучение сотрудников: развивать навыки соблюдения правил работы с коммерческой тайной и повышать уровень осведомленности о последствиях за их нарушения

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для защиты коммерческой тайны посредством выявления инцидентов ИБ и анализа событий безопасности необходимо использовать решения, которые:

- Позволяют выявлять угрозы и инциденты, приводящие к утечке коммерческой тайны
- Помогают управлять доступом пользователей к информации, относящейся к коммерческой тайне
- Позволяют отслеживать действия сотрудников, имеющих доступ к коммерческой тайне
- Позволяют идентифицировать уязвимости, которые могут быть использованы для несанкционированного доступа к коммерческой тайне
- Обеспечивают защиту и восстановление данных в случае инцидентов

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)

Использование указанных сервисов позволяет значительно снизить риски утечек и несанкционированного доступа к конфиденциальной информации, а также способствовать созданию безопасной информационной среды, защищая коммерческие интересы организации

ФЗ № 224-ФЗ от 27.07.2010

О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации

Эмитенты | Профессиональные участники рынка ценных бумаг | Финансовые посредники | Финансовые регуляторы

Ключевые требования к выполнению нормативного акта

01 Определение инсайдерской информации: установление правил и процедур для определения и учета инсайдерской информации

02 Запрет на злоупотребление инсайдерской информацией: эмитенты и профессиональные участники рынка должны воздерживаться от совершения сделок с ценными бумагами на основании инсайдерской информации

03 Ограничение доступа к инсайдерской информации: разработка и внедрение внутренних регламентов по доступу к инсайдерской информации для сотрудников организаций

04 Мониторинг и контроль: ведение учета инсайдерской информации и осуществление внутреннего контроля для предотвращения манипуляций на рынке

05 Ответственность за нарушения: установление ответственности за неправомерное использование инсайдерской информации и манипулирование рынком, включая административные и уголовные меры

06 Обучение сотрудников: проведение для сотрудников обучающих мероприятий касающихся инсайдерской информации и законности ее использования

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для защиты инсайдерской информации посредством выявления инцидентов ИБ и анализа событий безопасности необходимо использовать решения, которые:

- Анализируют поведение сотрудников и выявляют аномалии, такие как несанкционированный доступ к конфиденциальной информации или необычные операции с ценными бумагами
- Помогают агрегировать логи и события, обеспечивая возможность их анализа в реальном времени для выявления признаков манипуляций
- Позволяют ограничивать доступ к инсайдерской информации
- Помогают оперативно реагировать на возникающие угрозы, минимизируя риск утечек и манипуляций
- Позволяют фиксировать действия пользователей с инсайдерской информацией и генерировать отчеты, необходимые для соблюдения законодательно установленных требований

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)

Использование указанных сервисов помогает создать систему защитных мер, соответствующих требованиям законодательства, обеспечить безопасность информации и доверие со стороны инвесторов и клиентов, снижая риск манипуляций на рынке

ФЗ № 187 от 26.07.2017

О безопасности критической информационной инфраструктуры Российской Федерации

Энергетика | Финансовый сектор | Связь и телекоммуникации | Государственные и муниципальные органы | Водоснабжение и водоотведение | Обеспечение безопасности государства | Здравоохранение | Транспорт

Ключевые требования к выполнению нормативного акта

01 Идентификация объектов КИИ: проведение процедуры идентификации объектов, которые относятся к критической информационной инфраструктуре

02 Оценка угроз безопасности КИИ: проведение оценки рисков и угроз безопасности информационной инфраструктуры, включая уязвимости

03 Разработка и внедрение мер безопасности: определение и внедрение комплекса организационных и технических мер защиты КИИ

04 Обучение сотрудников: проведение регулярных обучающих мероприятий для работников организаций, обеспечивающих безопасность КИИ

05 Регулярный мониторинг и аудит: организация действий по мониторингу состояния безопасности КИИ и проведение регулярного аудита систем безопасности

06 Информирование об инцидентах: установление порядка информирования компетентных органов об инцидентах, угрожающих безопасности объектов КИИ

07 Разработка планов реагирования на инциденты: создание и внедрение планов реагирования на инциденты информационной безопасности, включая действия по минимизации ущерба

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для реализации мер по безопасности КИИ, взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак необходимо использовать решения, которые:

- Собирают и анализируют события безопасности в реальном времени, позволяя выявлять атаки на критическую инфраструктуру
- Помогают выявить слабые места в системах безопасности и адаптировать меры защиты
- Контролируют доступ сотрудников к критически важной информации и ресурсам, что способствует предотвращению несанкционированного доступа
- Автоматизируют процессы реагирования на инциденты, что повышает его оперативность и снижает риски
- Фиксируют все действия, связанные с управлением критической информацией, что является обязательным условием для соблюдения законодательства

Сервисы JSOC, соответствующие требованиям регуляторов

- Мониторинг АСУ ТП и объектов КИИ
- Сервисы ГосСОПКА
- Управление процессами реагирования на киберинциденты (IRP)

Использование сервисов обеспечивает целостность и защиту критической информационной инфраструктуры от потенциальных рисков и инцидентов. Это создает основу для безопасного функционирования и устойчивости критически важных объектов

Указ Президента РФ № 250 от 01.05.2022

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

ФОИВы | Государственные учреждения | Стратегические предприятия | Системообразующие организации | Субъекты КИИ

Ключевые требования к выполнению нормативного акта

01 Сертификация средств информационной безопасности: все средства информационной безопасности, специальные технические средства и системы, используемые для защиты КИИ, должны пройти процедуру сертификации на соответствие требованиям безопасности

02 Соотнесение с тарифами и нормами: необходимо соответствовать установленным тарифам и нормативам на услуги по сертификации и проведению испытаний средств ИБ для обеспечения защиты КИИ

03 Обеспечение соответствия требованиям: организации, работающие с КИИ, обязаны использовать только сертифицированные средства защиты для минимизации рисков

04 Организация аудита: аудит систем безопасности является важной частью проверки соответствия требованиям и обеспечивает возможность оценки уровня защиты

05 Обучение и повышение квалификации: сотрудники, работающие с информационными системами и средствами ИБ, должны проходить обучение и повышать свою квалификацию в соответствующей области

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для реализации дополнительных мер по обеспечению информационной безопасности государственных и стратегических предприятий необходимо использовать решения, которые:

- Позволяют оперативно выявлять аномальные события и инциденты в реальном времени, что критически важно для безопасности КИИ
- Обеспечивают анализ данных и корреляцию событий, что помогает оценить риски и потенциальные угрозы для КИИ
- Помогают контролировать соблюдение установленных политик безопасности в отношении использования сертифицированных средств защиты
- Автоматизируют реагирование на инциденты, что позволяет быстро принимать меры по устранению угроз и минимизации последствий
- Предоставляют необходимую документацию для рыночного и государственного регулирования
- Повышают уровень осведомленности работников о важности соблюдения стандартов безопасности

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Мониторинг АСУ ТП и объектов КИИ

Использование сервиса минимизирует риски, связанные с угрозами и инцидентами. Эффективные системы безопасности, соответствующие сертифицированным стандартам, играют ключевую роль в обеспечении защиты информации

Приказ ФСТЭК России № 235 от 21.12.2017

Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ и обеспечению их функционирования

Энергетика | Финансовый сектор | Водоснабжение и водоотведение | Связь и телекоммуникации | Здравоохранение | Транспорт

Ключевые требования к выполнению нормативного акта

01 Создание систем безопасности: системы безопасности должны быть разработаны для всех значимых объектов КИИ и включать правовые, организационные и технические меры по обеспечению информационной безопасности

02 Обеспечение устойчивого функционирования: системы безопасности предназначены для предотвращения неправомерного доступа и воздействия на технические средства, а также для восстановления функционирования объектов при атаках

03 Создание организационно-распорядительных документов: необходимо разработать и внедрить организационно-распорядительные документы по обеспечению безопасности значимых объектов, регламентирующие действия внутри организации

04 Поддержание квалификации персонала: работники, ответственные за безопасность, должны иметь соответствующее образование и опыт работы в области информационной безопасности

05 Планирование мероприятий по безопасности: следует разработать и утвердить планы мероприятий по обеспечению безопасности, включая планы реагирования на инциденты

06 Мониторинг и аудит: необходимо установить регулярный контроль и аудит систем безопасности для обеспечения их эффективности и соответствия установленным требованиям

07 Использование сертифицированных средств защиты: для обеспечения безопасности должны использоваться средства защиты информации, сертифицированные в соответствии с нормативными актами

08 Взаимодействие с государственной системой безопасности: системы безопасности должны обеспечить взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для выполнения требований по обеспечению безопасности значимых объектов КИИ необходимо использовать решения ИБ, которые:

- Позволяют собирать и анализировать события в реальном времени, что помогает быстро выявлять и реагировать на инциденты безопасности
- Помогают организовать процессы реагирования, минимизируя ущерб от инцидентов
- Позволяют своевременно выявлять и устранять слабые места в системах, что непосредственно соответствует требованиям поддержания безопасности
- Помогают следить за действиями сотрудников и предотвращать неправомерный доступ к критическим информационным ресурсам
- Позволяют повысить уровень осведомленности сотрудников о киберугрозах и процедурах безопасности, что способствует выполнению требований приказа
- Предоставляют задокументированные сведения обо всех действиях по мониторингу, анализу и реагированию на инциденты, что соответствует требованиям о ведении учета и отчетности

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)

Использование указанных сервисов помогает организациям защищать значимые объекты критической информационной инфраструктуры через реализацию эффективных мер безопасности

Приказ ФСТЭК России № 239 от 25.12.2017

Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ

Государственные и частные организации, которые управляют или используют значимые объекты КИИ

Ключевые требования к выполнению нормативного акта

01 Анализ угроз безопасности информации: выявление и оценка возможных угроз безопасности информации для каждого значимого объекта. Проведение анализа уязвимостей объектов и разработка моделей угроз

02 Разработка организационных и технических мер: установление правил и процедур идентификации и аутентификации пользователей и устройств. Реализация контроля доступа к объектам защиты. Защита информации на машинных носителях

03 Реализация системы защиты информации: использование сертифицированных средств защиты информации не ниже установленного уровня. Обеспечение антивирусной защиты и защиты от компьютерных атак

04 Аудит и мониторинг безопасности: проведение регулярного аудита безопасности значимых объектов. Настройка систем мониторинга для отслеживания безопасности и анализа событий

05 Планирование мероприятий по реагированию на инциденты: разработка и внедрение процедур реагирования на инциденты. Обучение персонала действиям в случае возникновения нештатных ситуаций

06 Документирование мероприятий по безопасности: регистрация результатов анализа угроз, мероприятий по безопасности и инцидентов. Оформление проектной и эксплуатационной документации, регламентирующей меры безопасности

07 Соблюдение законодательства: принятие мер в соответствии с российским законодательством о защите информации, государственной тайне и безопасности критической информационной инфраструктуры

08 Обеспечение безопасности при выводе из эксплуатации: архивирование и уничтожение (стирание) информации в случае завершения работы значимого объекта

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для обеспечения безопасности значимых объектов КИИ необходимо использовать решения ИБ, которые:

- Прошли обязательную сертификацию на соответствие требованиям по безопасности, установленным нормами и стандартами. В зависимости от категории значимости объекта должны применяться средства не ниже определенного уровня защиты (например, 4, 5 или 6 класс защиты)
- Предлагают многоуровневую защиту, включая защиту на аппаратном, программном и сетевом уровнях, а также средства защиты для виртуализированных сред
- Поддерживают функции управления доступом, включая идентификацию и аутентификацию пользователей, а также контроль и управление учетными записями
- Предоставляют средства для аудита безопасности и мониторинга событий безопасности, включая ведение журналов и анализ сетевого трафика
- Предоставляют защиту от различных типов атак
- Регулярного производят обновления и устанавливают патчи для устранения уязвимостей. Гарантируют техническую поддержку
- Включают функции криптографической защиты информации, сохраняя конфиденциальность, целостность и аутентичность данных
- Содержат полную эксплуатационную документацию, включая инструкции по установке, настройке и использованию продукта, а также описания процедур по реагированию на инциденты

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Мониторинг АСУ ТП и объектов КИИ
- Анализ сетевого трафика (NTA)
- Сервисы ГосСОПКА

Использование таких сервисов способствует высокому уровню защищенности значимых объектов и помогает эффективно выполнять требования приказа

Приказ ФСБ России № 282 от 19.06.2019

Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации

Финансовые учреждения | Субъекты КИИ

Ключевые требования к выполнению нормативного акта

01 Информирование о компьютерных инцидентах: субъекты КИИ обязаны уведомлять ФСБ России обо всех компьютерных инцидентах, связанных с их объектами, в срок не позднее 3 часов с момента их обнаружения. Информация передается в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) с использованием предустановленных форматов

02 Разработка плана реагирования: субъекты обязаны разработать план реагирования на компьютерные инциденты в течение 90 дней с момента включения объекта в реестр значимых объектов. План должен включать технические характеристики объектов, условия запуска мероприятий, список ответственных подразделений и должностных лиц

03 Ежегодные тренировки: субъекты должны проводить ежегодные тренировки по отработке мероприятий по реагированию на инциденты для обеспечения готовности к выполнению плана

04 Координация с Банком России: если инцидент связан с объектом в банковской сфере или на финансовом рынке, информация также передается в Банк России с соблюдением установленных сроков

05 Анализ инцидентов: субъекты должны анализировать инциденты для определения связи с компьютерными атаками и очередности их устранения, реализуя мероприятия в соответствии с разрабатываемым планом

06 Уведомление о результатах: по завершении мероприятий по реагированию и ликвидации последствий субъект должен сообщать НКЦКИ об их результатах в срок не позднее 48 часов

07 Привлечение подразделений ФСБ: в план может быть включена возможность привлечения подразделений ФСБ к реагированию на инциденты и ликвидации их последствий

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для соответствия требованиям приказа решения информационной безопасности должны включать:

- Системы мониторинга, которые позволяют оперативно выявлять компьютерные инциденты и угрозы, что содействует быстрому реагированию
- Средства сбора и хранения информации об инцидентах, что способствует более качественному информированию ФСБ и других заинтересованных органов
- Инструменты анализа инцидентов и возможность инициировать необходимые действия по ликвидации последствий атак, обеспечивая выполнение мероприятий, прописанных в плане реагирования
- Инструменты для проведения тренировок и учений по реагированию на инциденты, что повышает эффективность подготовки персонала

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Мониторинг АСУ ТП и объектов КИИ
- Сервисы ГосСОПКА

Использование указанных сервисов способствуют созданию более безопасной киберсреды и соответствию требованиям законодательства в области кибербезопасности

Приказ ФСБ России № 367 24.07.2018

Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Субъекты КИИ | Финансовые учреждения

Ключевые требования к выполнению нормативного акта

01 Информирование о компьютерных инцидентах: субъекты КИИ обязаны сообщать о всех компьютерных инцидентах, связанных с их объектами, в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) не позднее 24 часов с момента их обнаружения

02 Перечень предоставляемой информации: данные о значимых объектах КИИ; информация о присвоении или изменении категории значимости объекту; сведения о нарушениях требований безопасности, которые могут стать причиной компьютерных инцидентов; данные о компьютерных инцидентах, включая дату, время, место, технические параметры и последствия инцидента

03 Порядок представления информации: информация должна быть представлена независимо от того, подключен ли субъект к технической инфраструктуре НКЦКИ. Если подключения нет, информация может быть отправлена с помощью факса, почтовой или электронной связи. Вся информация должна направляться в соответствии с определенными НКЦКИ форматами

04 Частота и сроки: информация, указанная в пунктах 1–4 Перечня, должна отправляться не реже одного раза в месяц и в установленные сроки. В случае существенных изменений в статусе объектов КИИ, например, включение в реестр или изменение его категории

05 Поддержание готовности: субъекты должны вести систематическую работу по выявлению, предупреждению и ликвидации последствий компьютерных атак, а также регулярно проверять и обновлять процедуры и технологии безопасности

06 Соответствие законодательству: все действия и представляемая информация должны соответствовать требованиям законодательства о безопасности критической информационной инфраструктуры

Требования к решениям ИБ в части мониторинга и реагирования на инциденты ИБ

Для соответствия требованиям приказа решения информационной безопасности должны:

- Обеспечивать постоянный контроль за состоянием сетевой и информационной инфраструктуры, подписывать и анализировать логи событий безопасности
- Определять и предотвращать атаки на стадии их возникновения
- Иметь возможность для автоматической обработки инцидентов, включая использование заранее подготовленных сценариев реагирования
- Генерировать отчеты о событиях и инцидентах безопасности, которые соответствуют установленным требованиям и стандартам и сохраняются для последующего анализа и аудита
- Осуществлять обмен данными и автоматически передавать информацию в НКЦКИ или другие контролирующие органы
- Поддерживать возможность для проведения регулярных внутренних проверок на соответствие требованиям и работоспособность систем мониторинга и реагирования
- Содержать материалы для обучения персонала
- Соответствовать действующим стандартам по информационной безопасности

Сервисы JSOC, соответствующие требованиям регуляторов

- Сервис мониторинга и анализа инцидентов (SOC)
- Мониторинг АСУ ТП и объектов КИИ
- Сервисы ГосСОПКА

Использование сервисов создает надежную защиту для организаций и их критической информационной инфраструктуры