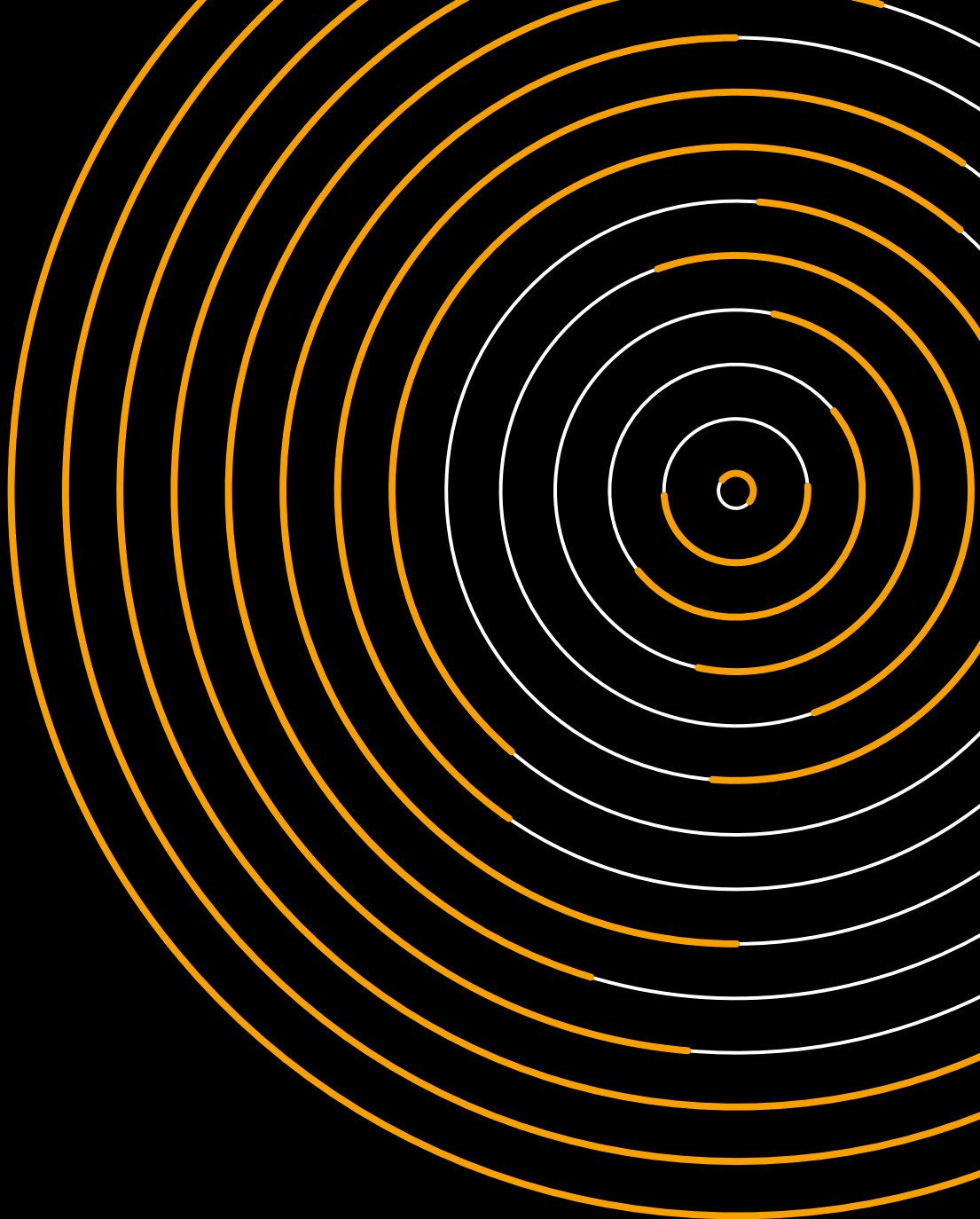




Security Operations Center

**Как выполнить требования 187-ФЗ
в части подключения к ГосСОПКА**

[SOC.USSC.RU](https://soc.ussc.ru)

Что такое ГосСОПКА?

ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации. Координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению компьютерных атак, организует сбор и обмен информацией об инцидентах между субъектами критической информационной инфраструктуры (КИИ) – Национальный координационный центр по компьютерным инцидентам (НКЦКИ)

Что такое ФинЦЕРТ?

ФинЦЕРТ – это центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специальное структурное подразделение Банка России

Обязательно ли подключение субъектов КИИ и ГосСОПКА и ФинЦЕРТ?

Статья 9. 187-ФЗ

Субъект КИИ обязан незамедлительно информировать о компьютерных инцидентах в соответствующие федеральные органы исполнительной власти (НКЦКИ, а также ФинЦЕРТ ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке

Статья 10. 187-ФЗ, Приказы ФСТЭК России №235 и №239

Системы безопасности значимых объектов КИИ должны обеспечивать непрерывное взаимодействие с ГосСОПКА

Приказ ФСБ России №282

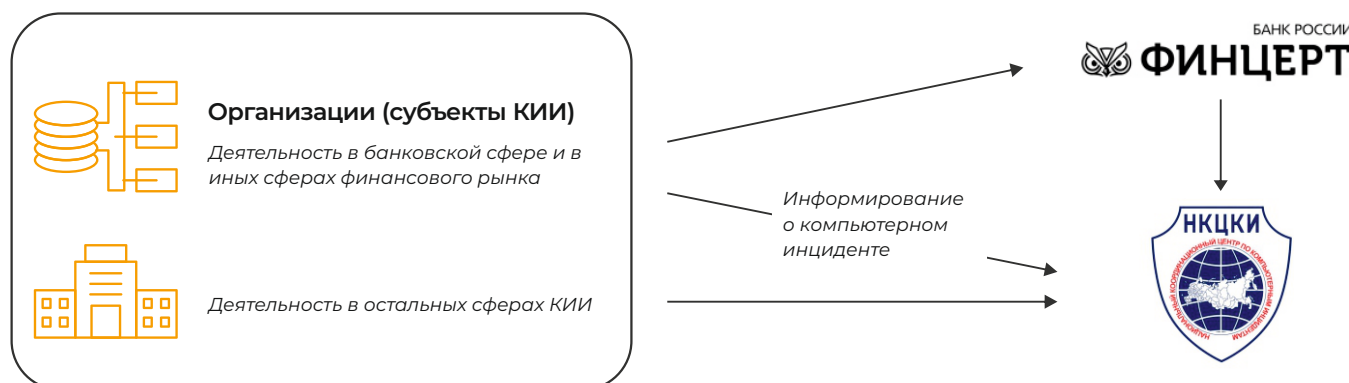
Субъект КИИ обязан направить информацию о компьютерном инциденте (КИ), связанном с функционированием значимого ОКИИ, в НКЦКИ (а также в ФинЦЕРТ ЦБ РФ для финансовых организаций) в срок не позднее 3 часов с момента обнаружения КИ, а в отношении ОКИИ – в срок не позднее 24 часов с момента его обнаружения

Приказы ФСБ России №367 и №282

Взаимодействие с НКЦКИ осуществляется с использованием технической инфраструктуры (ТИ) НКЦКИ, с ФинЦЕРТ – с использованием ТИ Банка России или посредством почтовой, факсимильной или электронной связи

Статья 274.1 УК РФ

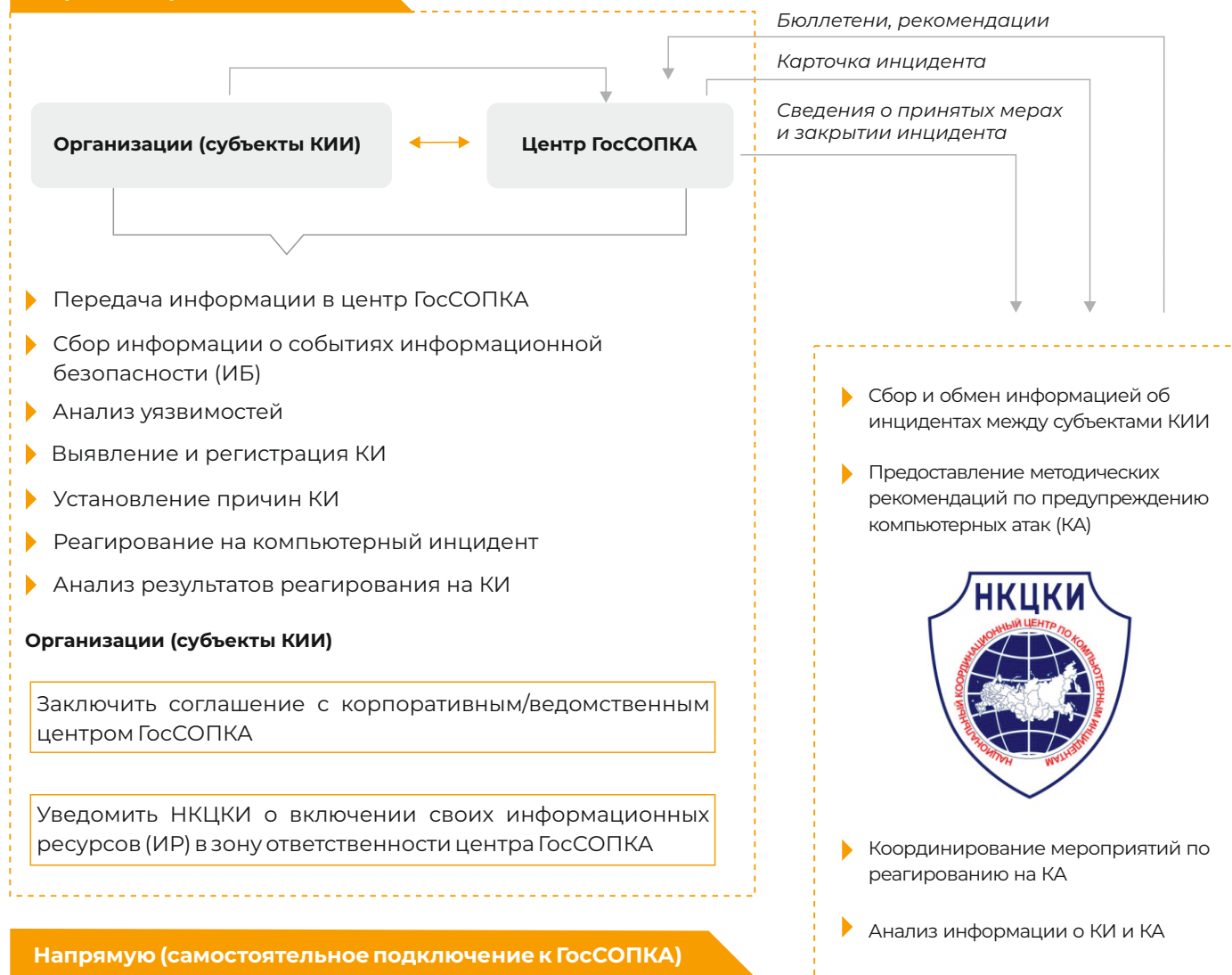
Нарушение правил эксплуатации, либо правил доступа к объектам КИИ, повлекшее тяжкие последствия, грозит лишением свободы до 10 лет



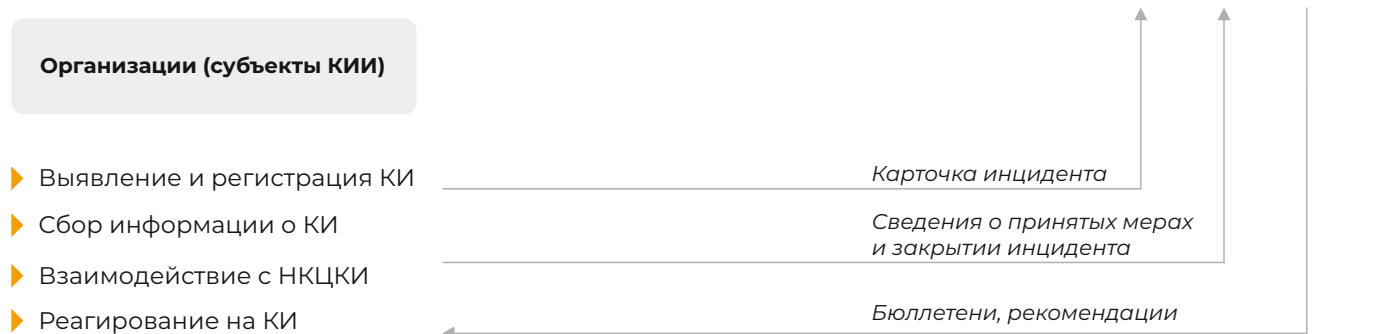
Все субъекты КИИ, независимо от владения значимыми объектами КИИ, обязаны информировать НКЦКИ о компьютерных инцидентах

Варианты взаимодействия субъектов КИИ с НКЦКИ

Через Центр ГосСОПКА



Напрямую (самостоятельное подключение к ГосСОПКА)



Организации (субъекты КИИ)

Направить письменный запрос в ФСБ России о подключении к ГосСОПКА с указанием сферы деятельности субъекта КИИ, перечня ИР, включенных в зону ответственности субъекта КИИ, контактных данных лиц, ответственных за взаимодействие

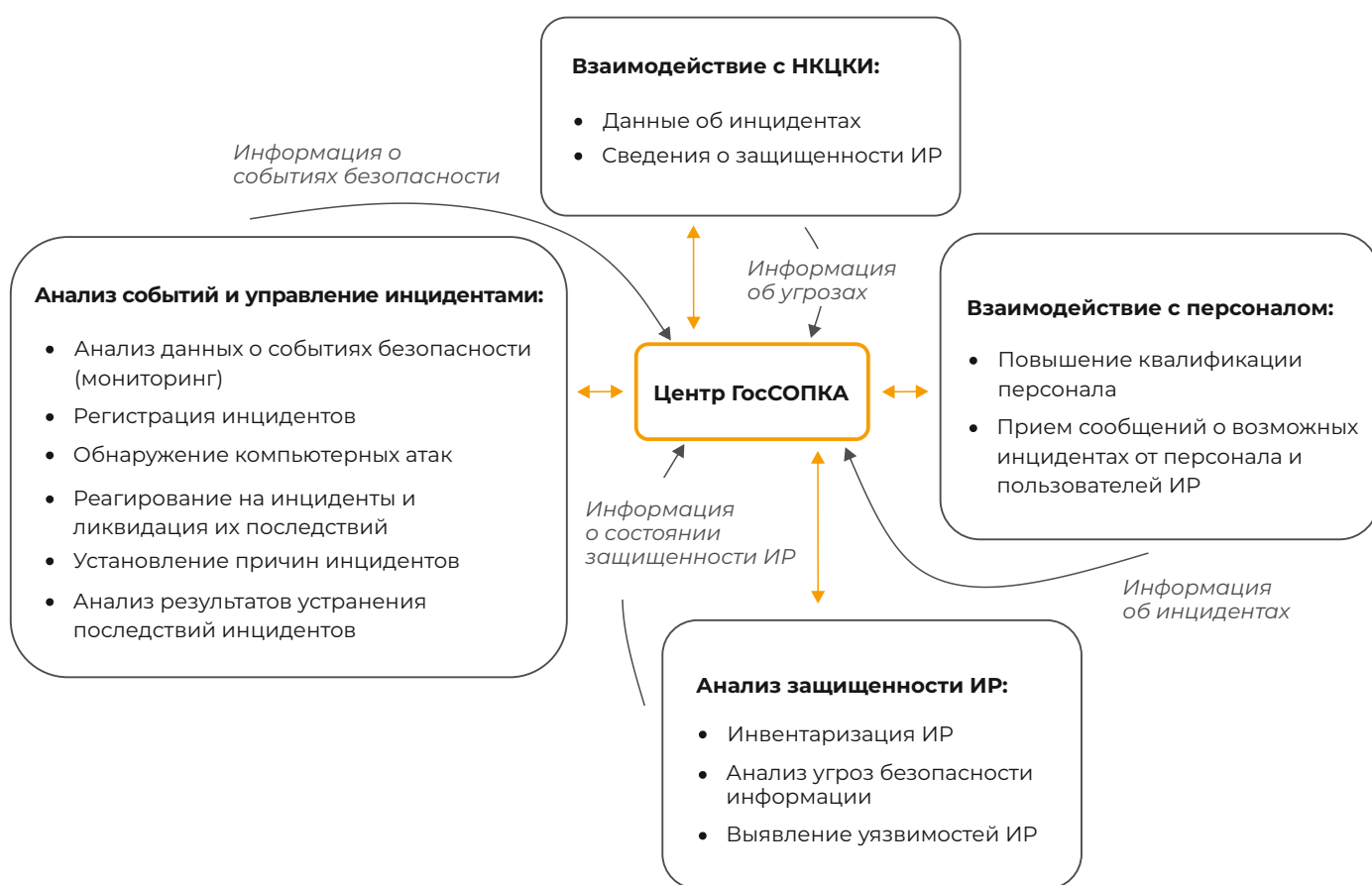
Обеспечить наличие необходимых ресурсов: персонала, средств обнаружения, предотвращения и ликвидации последствий компьютерных атак

Подготовить необходимую организационно-распорядительную документацию в соответствии с нормативными правовыми актами и методическими рекомендациями

Организовать специализированную систему взаимодействия и подключить организацию к технической инфраструктуре НКЦКИ под определенной учетной записью (обязательно для значимых ОКИИ)

Согласно документу ФСБ России «Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА» задачами центра ГосСОПКА являются:

- ▶ Обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы
- ▶ Проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы
- ▶ Сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах
- ▶ Осуществление взаимодействия между центрами по вертикали иерархической структуры ГосСОПКА
- ▶ Информирование в зоне ответственности субъекта ГосСОПКА заинтересованных лиц по вопросам обнаружения, предупреждения и ликвидации последствий контролируемых атак
- ▶ Формирование и поддержание в актуальном состоянии информации о контролируемых ресурсах



Дополнительно, при наличии соглашения о взаимодействии Центра ГосСОПКА с ЦБ РФ по вопросу противодействия компьютерным атакам, возможно осуществление взаимодействия между участниками информационного обмена с Банком России через защищенный портал – осуществление взаимодействия с автоматизированной системой сбора и обработки информации (АСОИ) ФинЦЕРТ

Деятельность центра ГосСОПКА может обеспечиваться:

- ▶ Путем назначения соответствующих ролей работникам структурных подразделений организации
- ▶ Путем заключения договоров со специализированными организациями – корпоративными центрами ГосСОПКА, осуществляющими лицензируемую деятельность в области защиты информации и мониторинга ИБ средств и систем информатизации

Какие меры могут быть реализованы при подключении субъекта КИИ к центру ГосСОПКА?

Приказ ФСТЭК России №239
Меры по обеспечению безопасности для значимого объекта КИИ

Обозн/№	Меры обеспечения безопасности значимого объекта
Аудит безопасности (АУД)	
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.3	Генерирование временных меток и (или) синхронизация системного времени
АУД.4	Регистрация событий безопасности
АУД.5	Контроль и анализ сетевого трафика
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.9	Анализ действий отдельных пользователей
Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.3	Анализ компьютерных инцидентов
ИНЦ.4	Устранение последствий компьютерных инцидентов
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах

Обозн/№	Содержание мер системы защиты информации
---------	--

Подпроцесс «Обнаружение инцидентов защиты информации и реагирования на них»

РИ.1	Регистрация информации о событиях защиты информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации
РИ.2	Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов финансовой организации
РИ.10	Своевременное (оперативное) оповещение членов ГРИЗИ о выявленных инцидентах защиты информации
РИ.15	Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации
РИ.16	Разграничение доступа членов ГРИЗИ к информации об инцидентах защиты информации в соответствии с определенным распределением ролей, связанных с реагированием на инциденты защиты информации
РИ.17	Обеспечение возможностей доступа к информации об инцидентах защиты информации в течение трех лет
РИ.18	Обеспечение возможностей доступа к информации об инцидентах защиты информации в течение пяти лет
РИ.19	Регистрация доступа к информации об инцидентах защиты информации

Подпроцесс «Мониторинг и анализ событий защиты информации»

МАС.1	Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации
МАС.2	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевым оборудованием, в том числе, активным сетевым оборудованием, маршрутизаторами, коммутаторами
МАС.3	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевыми приложениями и сервисами
МАС.4	Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД
МАС.5	Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями
МАС.6	Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов
МАС.7	Организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами (системами) контроля и управления доступом

Подпроцесс «Мониторинг и анализ событий защиты информации»

МАС.8	Централизованный сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации
МАС.9	Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования сбора и анализа данных регистрации
МАС.10	Контроль формирования данных регистрации о событиях защиты информации объектов информатизации
МАС.11	Реализация защиты данных регистрации о событиях защиты информации от раскрытия и модификации, двухсторонней аутентификации при передаче данных регистрации с использованием сети Интернет
МАС.12	Обеспечение гарантированной доставки данных регистрации о событиях защиты информации при их централизованном сборе
МАС.13	Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации
МАС.14	Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечении целостности и доступности хранимых данных регистрации
МАС.16	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет
МАС.17	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет

Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

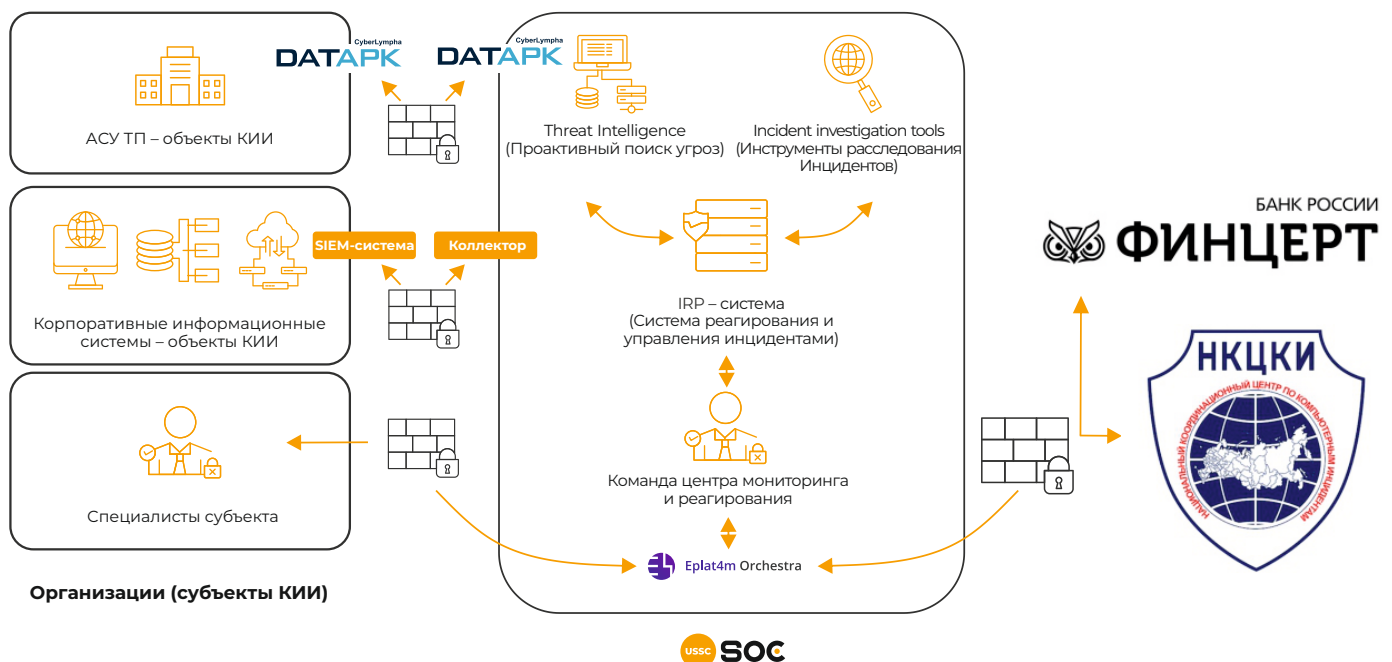
УЗП.22	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящее к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации
УЗП.23	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации клиентов и контрагентов
УЗП.24	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом
УЗП.25	Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектами логического доступа
УЗП.26	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию
УЗП.27	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации
УЗП.28	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами

USSC-SOC – корпоративный центр ГосСОПКА

Подключение к USSC-SOC позволит:

- ▶ Предотвращать киберугрозы путем непрерывного мониторинга компьютерных сетей на предмет наличия уязвимостей и анализа инцидентов безопасности
- ▶ Оперативно реагировать на подтвержденные инциденты и исключать ложные срабатывания
- ▶ Получать отчеты о состоянии безопасности и киберинцидентах
- ▶ Взаимодействовать с НКЦКИ и ФинЦЕРТ (для финансовых организаций) при решении задач, касающихся обнаружения предупреждения и ликвидации последствий компьютерных атак
- ▶ Обеспечить круглосуточный контроль за безопасностью организации в режиме 24x7
- ▶ Обеспечить централизацию обработки и хранения сведений о вторжениях и киберугрозах
- ▶ Снижать затраты организации на кибербезопасность (в долгосрочной перспективе)
- ▶ Сокращать ущерб и финансовые потери организации за счет оперативного реагирования на инциденты информационной безопасности
- ▶ Привлекать квалифицированный персонал в расследовании инцидентов
- ▶ Применять в процессе анализа событий постоянно пополняющиеся базы уязвимостей, актуальных угроз
- ▶ Автоматизировать действия администраторов по реагированию на инциденты информационной безопасности посредством плейбуков SOAR, разрабатываемых с учетом конкретной инфраструктуры
- ▶ Обеспечить быстрый запуск услуг по мониторингу и реагированию на инциденты информационной безопасности без долгосрочного бюджетирования и проектирования
- ▶ Проводить анализ существующих защитных мер и получать рекомендации по их корректировке
- ▶ Получить методическую поддержку в актуализации плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак для согласования их с ФСБ России (и Банком России – для финансовых организаций)

Архитектура взаимодействия субъектов КИИ с НКЦКИ и ФинЦЕРТ ЦБ РФ (для финансовых организаций)



Security Operation Center (SOC) – центр мониторинга и реагирования на инциденты информационной безопасности (центр ГосСОПКА)

Услуги, предоставляемые USSC-SOC

- ▶ Мониторинг, реагирование и расследование инцидентов ИБ в ИТ-инфраструктуре и промышленных (технологических) системах. В составе пакета услуг возможно предоставление в аренду средств сбора событий ИБ, контроля конфигурации (настроек) и анализа сетевого трафика
- ▶ Проектирование и внедрение центров мониторинга и реагирования на инциденты ИБ Security Operations Center (SOC), специализированных с учетом особенностей конкретного Заказчика, включая полную информационную поддержку при построении собственного SOC
- ▶ Автоматизация процессов реагирования на инциденты ИБ на стороне Заказчика с применением SOAR
- ▶ Обслуживание и сопровождение эксплуатации систем безопасности центров мониторинга и реагирования на инциденты ИБ, включая услуги по аудиту, поддержанию и развитию существующих центров мониторинга и реагирования на инциденты ИБ
- ▶ Реализация функций центра ГосСОПКА для субъектов КИИ, включая передачу информации в НКЦКИ



Центр ГосСОПКА за

2 месяца

Запустим базовые функции
корпоративного центра
ГосСОПКА менее, чем за 2 месяца



Варианты обслуживания

8x5

с 9:30 до 18:30 в рабочие дни

10x5

с 8:00 до 19:00 в рабочие дни

24x7

круглосуточно



Время реагирования
на инцидент

<60 мин

Преимущества USSC-SOC

- ▶ Является корпоративным центром ГосСОПКА класса А (выполняет самостоятельно полный комплект мероприятий в рамках реализации функций центра ГосСОПКА)
- ▶ Соответствует требованиям законодательства РФ в области ИБ
- ▶ Обладает лицензией ФСТЭК России на мониторинг ИБ средств и систем информатизации
- ▶ Подключен к НКЦКИ и ФинЦЕРТ
- ▶ Средства SOC (технические, программные, программно-аппаратные, криптографические) соответствуют требованиям Приказа ФСБ России №196
- ▶ MSSP-партнер компании Group-IB по направлению «Threat Intelligence & Attribution»

Экспертный опыт

- ▶ Стратегическая команда с глобальным видением, способная адаптировать методы защиты для различных индустрий
- ▶ Экспертиза в области защиты АСУ ТП
- ▶ В штате УЦСБ – сотрудники с высшим профессиональным образованием по направлению подготовки «Информационная безопасность», имеющие сертификаты (дипломы): Certified Information System Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Master of Business Administration (MBA), Certified Information Security Manager (CISM)

Соответствие нормативным требованиям

- ▶ Все работы проводятся в соответствии с требованиями законодательства и методическими рекомендациями ФСБ России
- ▶ УЦСБ является лицензиатом ФСТЭК России и ФСБ России
- ▶ Обеспечение Service Level Agreement (SLA)

Передовые технологии

- ▶ Прогнозирование сложных угроз информационной безопасности, скрывающихся за незначительными инцидентами
- ▶ Работа без установки дополнительного ПО на компоненты АСУ ТП
- ▶ Использование SOAR для ускорения автоматизации процессов обработки инцидентов

Узнать подробнее

soc@ussc.ru

