USSC

Использование **Security Operations Center** в финансовых учреждениях

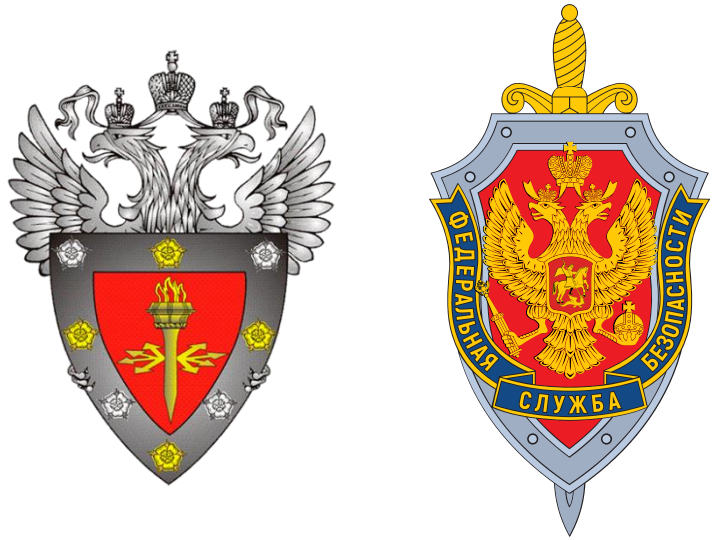
Руслан Амиров

Директор Центра мониторинга ИБ

USSC-SOC

Причины использования SOC

1. Внешние требования
2. Результаты оценки рисков
3. Предотвращение ущерба
4. Непрерывность ИТ-инфраструктуры и бизнес-процессов
5. Экономический аспект
6. Свой вариант



Банк России

Внешние требования

- Федеральный закон **187-ФЗ** «О безопасности критической информационной инфраструктуры РФ»
- Положения Банка России (**683-П, 684-П, 747-П, 719-П**)
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»
- Законодательство в области **защиты ПДн**
- **Требования ФСБ** России
- **Прочие НПА ЦБ РФ**

Топ 5 проблемных требований ГОСТ 57580.1-2017

01
Межсетевое экранирование во внутренней сети

02
Централизованный сбор событий безопасности

03
Обнаружение и регистрация инцидентов защиты информации

04
Требования по контролю

05
Учет машинных носителей информации

Ответственность за нарушение внешних требований

УК РФ Ст. 274.1. Неправомерное воздействие на КИИ РФ

До 10 лет лишения свободы
Нарушение правил эксплуатации либо правил доступа к объектам КИИ, если они повлекли тяжкие последствия

До 6 лет лишения свободы
Нарушение правил эксплуатации либо правил доступа к объектам КИИ

До 5 лет лишения права занимать определенные должности

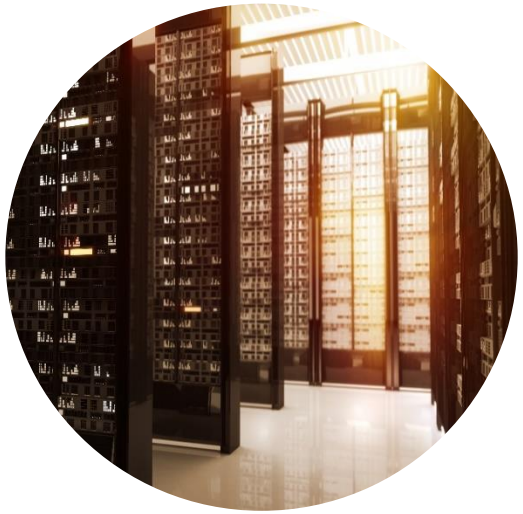
Изменения в КоАП РФ по вопросам безопасности КИИ

Штраф до 500 тыс. руб
Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ

Штраф до 100 тыс. руб
Нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования

Штраф до 500 тыс. руб
Непредставление или нарушение порядка либо сроков представления информации в ГосСОПКА

Основные варианты использования SOC



Привлечение **аутсорсингового SOC,** предоставляемого в качестве сервиса сторонней компанией, обладающей необходимыми компетенциями и лицензиями, в рамках договора с организацией

Использование **собственного SOC**, самостоятельно или с привлечением компетентной компании-интегратора

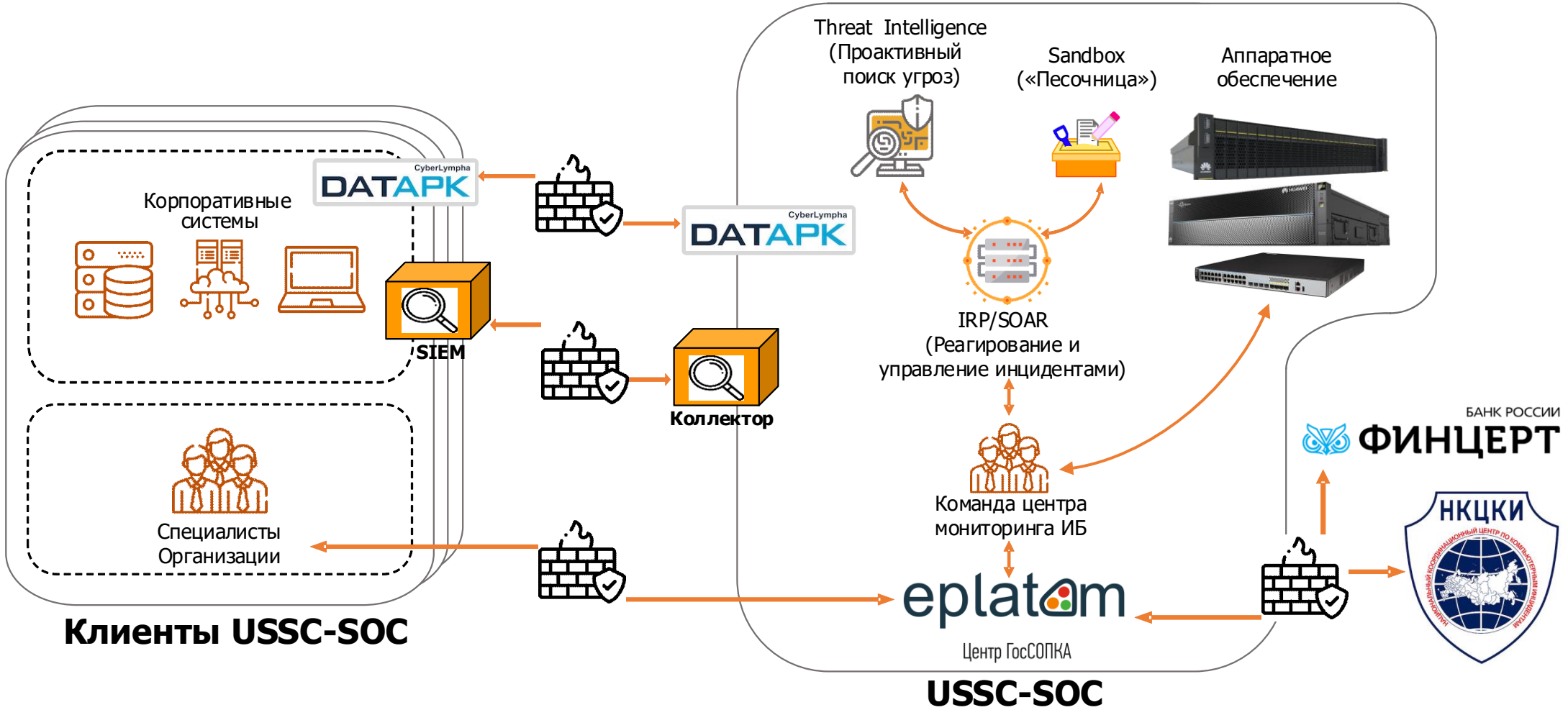
Основные варианты использования SOC

MSSP - Managed Security Service Provider
- предоставление управляемых сервисов по безопасности

MDR - Managed Detection and Response
- предоставление сервисов по обнаружению, реагированию и расследованию инцидентов ИБ

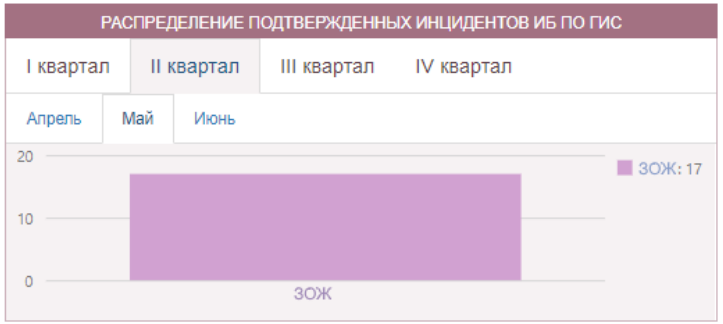
Использование **собственного SOC с использованием аутсорсинговых сервисов MSSP и MDR**, предоставляемых сторонней компанией, обладающей необходимыми компетенциями и лицензиями

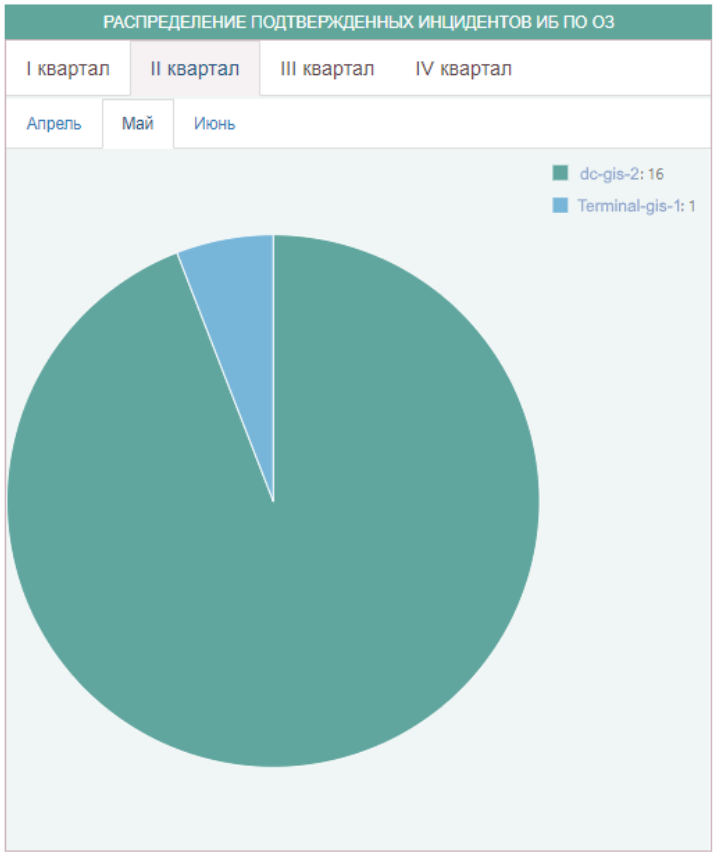
Архитектура SOC (на примере USSC-SOC)

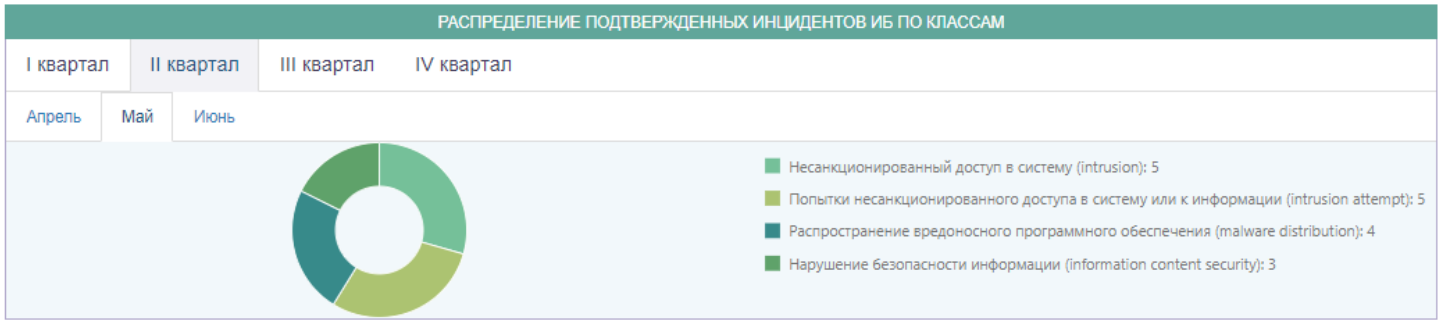


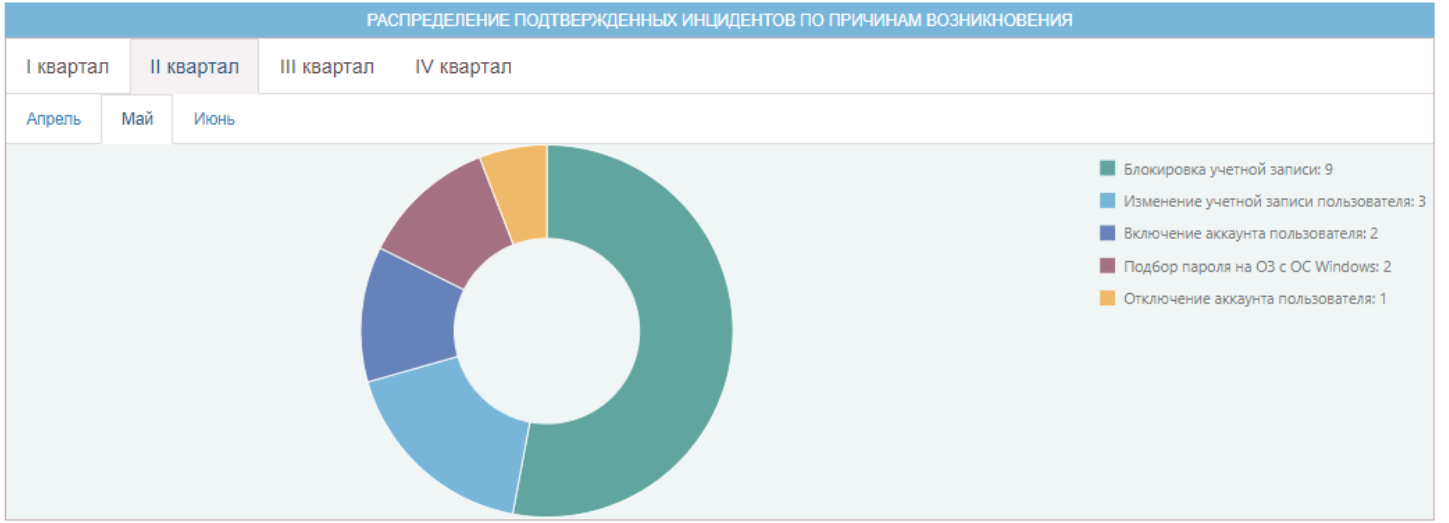
Дашборд Заказчика (подтвержденные инциденты)

USSC









Услуги УЦСБ

Аутсорсинговые услуги – USSC-SOC	Услуги для инфраструктуры существующего SOC
Предоставление услуг по мониторингу и реагированию на инциденты ИБ, долговременному хранению событий	Проектирование систем управления инцидентами ИБ (включая подключение к ГосСОПКА)
Взаимодействие с ГосСОПКА, ФинЦЕРТ	Модуль «Центр ГосСОПКА» eplat4m
Взаимодействие с CERT/CSIRT/SOC	Аудит, оптимизация существующего Security Operations Center

Проведение тестирований на проникновение, в том числе с использованием методов социальной инженерии

Расследование инцидентов информационной безопасности

Security Awareness (повышение осведомленности работников)

Как подключиться к SOC (на примере USSC-SOC)

USSC

1. **Отправить заявку** в свободной форме по адресу soc@ussc.ru, оставить обращение через сайт ussc.ru или просто позвонить по номеру +7 (343) 379-98-34. С Вами обязательно свяжутся и подробно проконсультируют
2. **Ответить на вопросы** инженера или заполнить опросный лист
3. **Подписать договор с УЦСБ** и регламент взаимодействия с USSC-SOC
4. **Встретить инженеров**, которые приедут и соберут нужную информацию для оказания услуги, установят и настроят оборудование
5. **Инвентаризировать** и (при необходимости) настроить **объекты мониторинга**
6. **Получить оповещение** о тестовом инциденте

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Вопросы по USSC-SOC можете направлять по адресу: soc@ussc.ru
Вам обязательно ответят!

Руслан Амиров
Директор Центра мониторинга ИБ
USSC-SOC
+7 (343) 379-98-34 (доб. 1203)
ramirov@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU