ГосСОПКА. Для кого же?

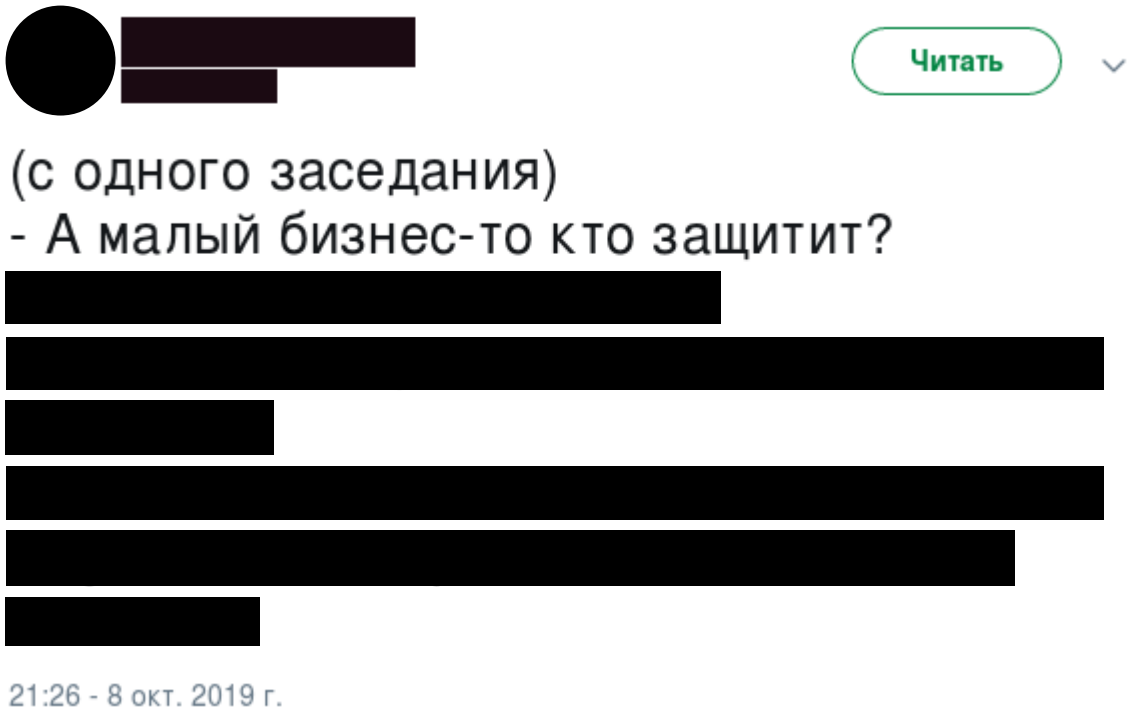
Сергей Корелов

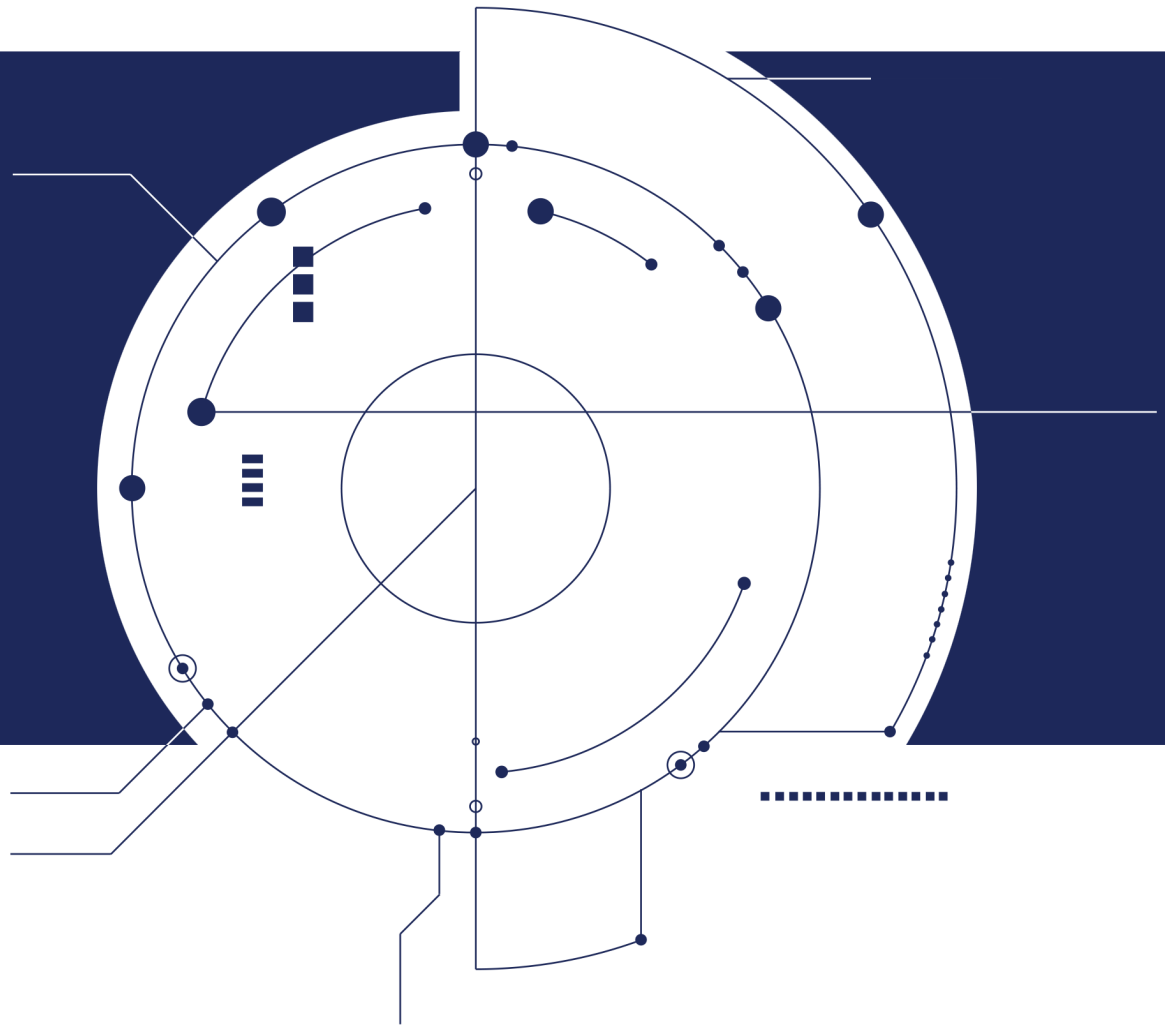
НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Почему об этом?





Так для кого же?

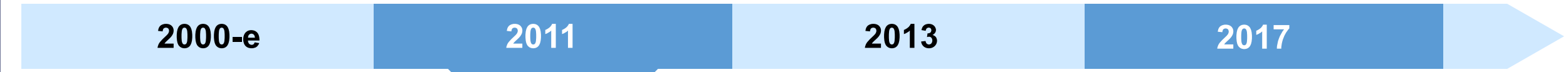
Этапы развития ГосСОПКА

2000-е | **2011** | **2013** | **2017**

Созданы и отработаны технологии и механизмы информационного взаимодействия при реагировании на компьютерные атаки, компьютерные инциденты и угрозы безопасности

Взаимодействие будет эффективнее при бóльшем количестве участников

Этапы развития ГосСОПКА



Создан Центр реагирования на компьютерные инциденты в органах государственной власти

- Выполняет роль национального CERT
- На его базе мы начали выстраивать систему взаимодействия

Этапы развития ГосСОПКА

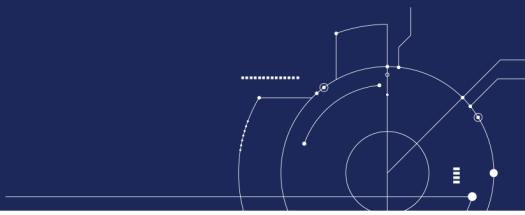
2000-е | **2011** | **2013** | **2017**

Указ Президента Российской Федерации от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

Введено понятие «информационные ресурсы РФ», закрепившее зону ответственности ГосСОПКА:

«информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом»

Этапы развития ГосСОПКА



2000-е | **2011** | **2013** | **2017**

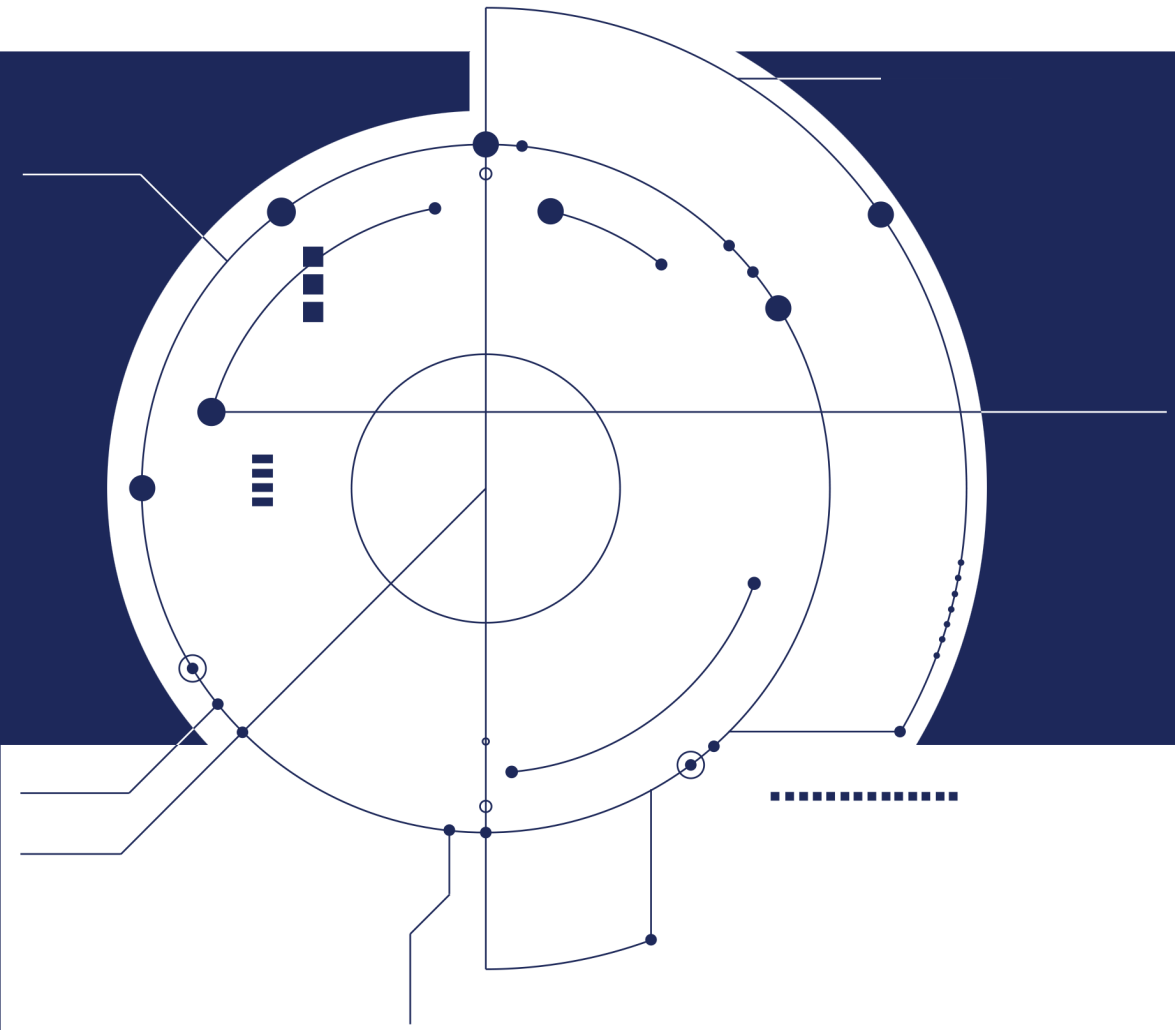
Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Уточнено и дополнено понятие «информационные ресурсы РФ»:

«информационные системы, информационно-телекоммуникационные сети **и автоматизированные системы управления**, находящиеся на территории Российской Федерации, ~~**и**~~ в дипломатических представительствах и **(или)** консульских учреждениях Российской Федерации ~~**за рубежом**~~»

Эффективность защиты

Чем больше участников вносят свой вклад в общую копилку знаний об угрозах и сами используют полученную информацию, тем эффективнее работает система



Что делать компаниям, не являющимся субъектами КИИ?

Ваша безопасность в Ваших руках

- Нормативные правовые акты в области защиты КИИ устанавливают требования и определяют тех, для кого выполнение данных требований является обязательным

- Остальные вправе выполнять соответствующие требования в добровольном порядке

Участники ГосСОПКА не только субъекты КИИ

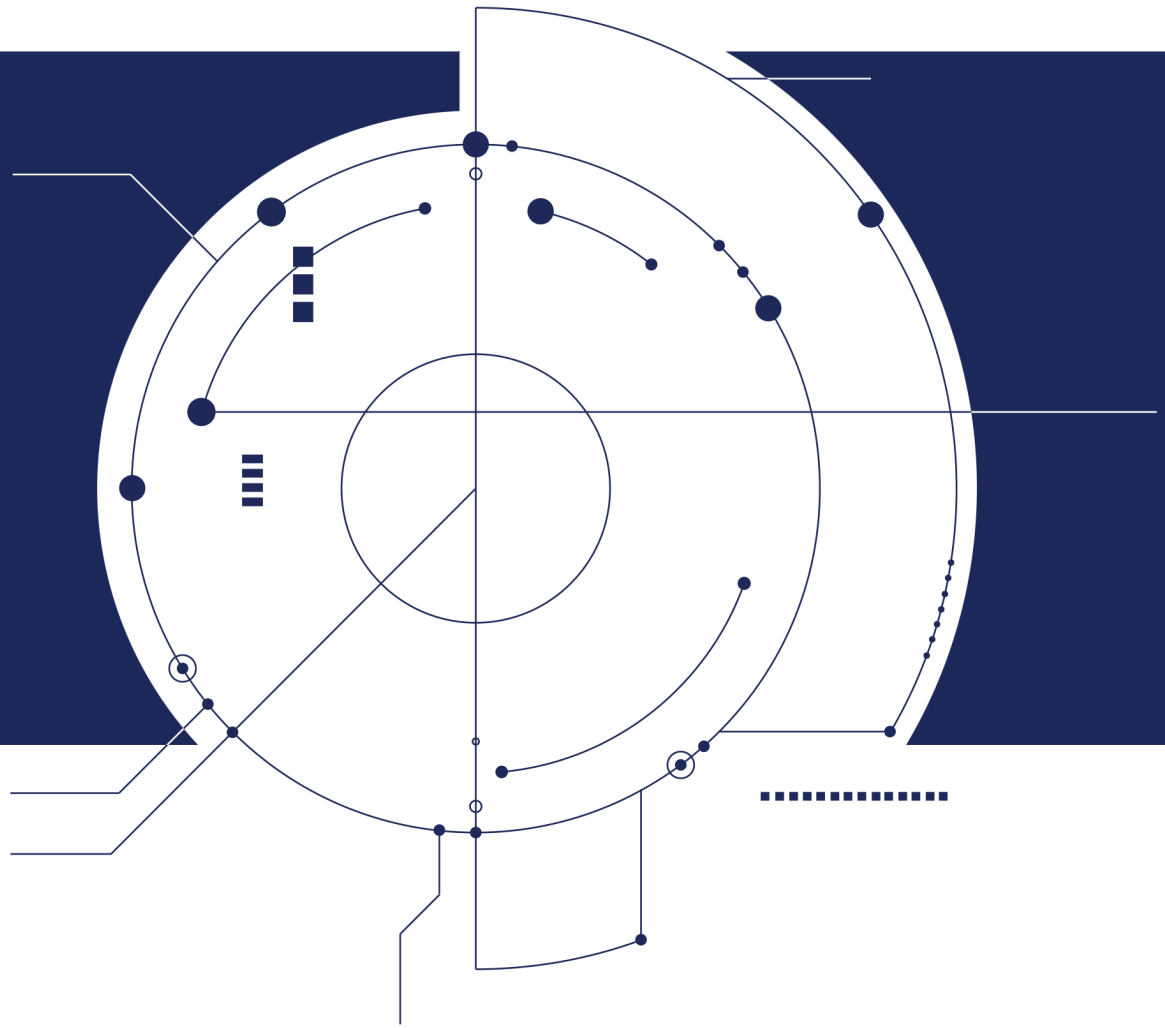
Мы открыты и готовы сотрудничать с теми,
кто чувствует ответственность за свой бизнес,
вне зависимости от того, относятся ли Ваши
информационные ресурсы к КИИ или нет

Монетизируйте возможные угрозы

Финансовые потери для бизнеса

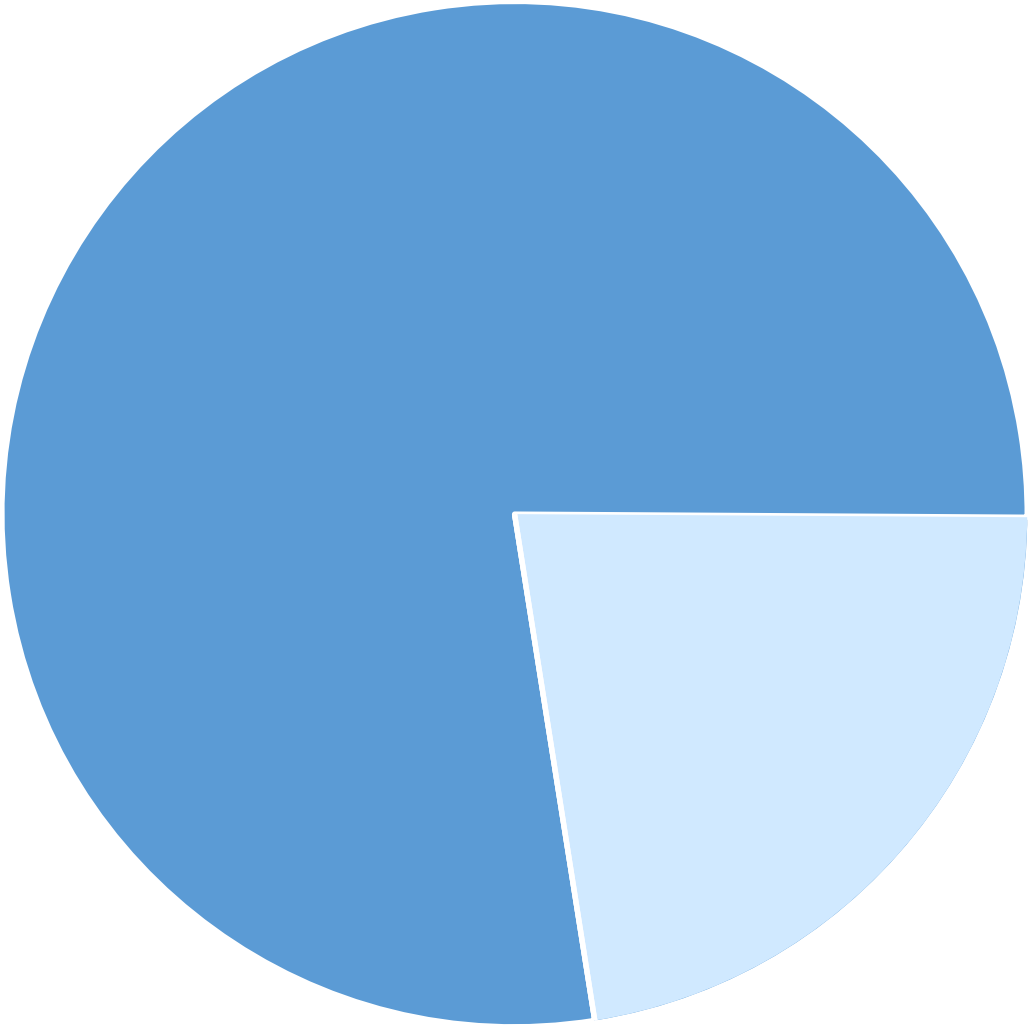
Угрозы информационным ресурсам

Будьте честны сами с собой



Что уже сделано?

Участники ГосСОПКА

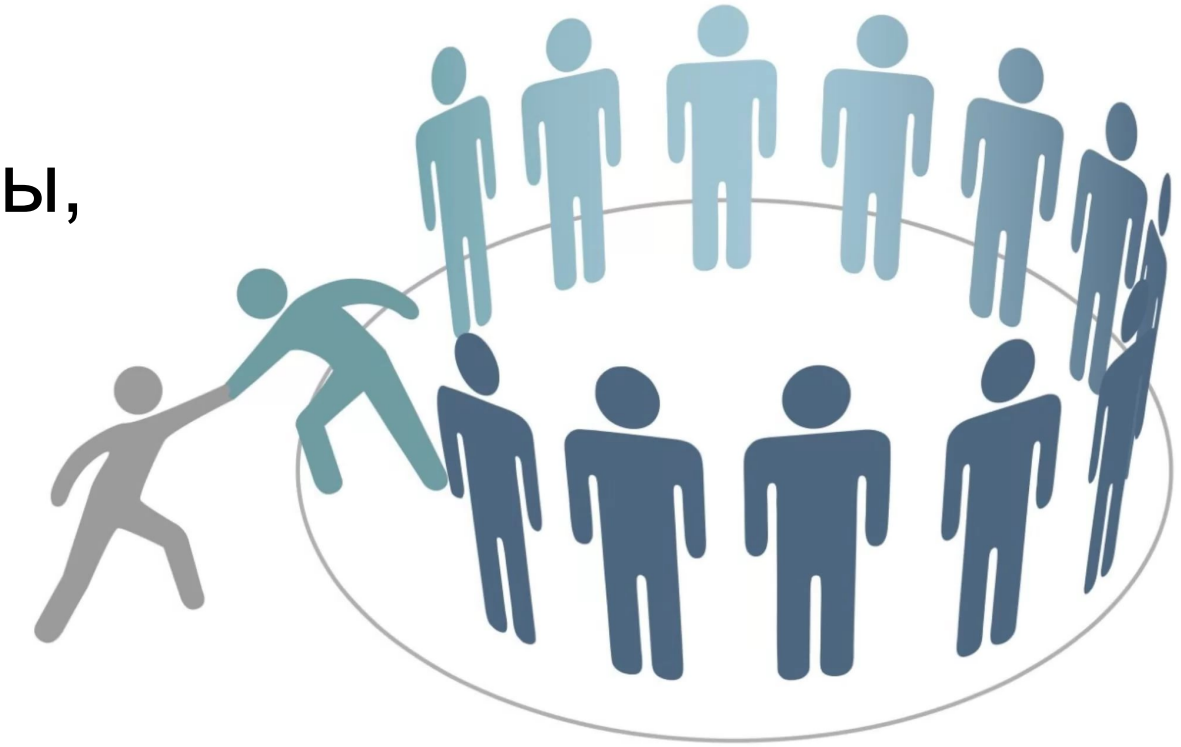


1853 субъекта ГосСОПКА

535 субъектов КИИ

Взаимодействие в ГосСОПКА

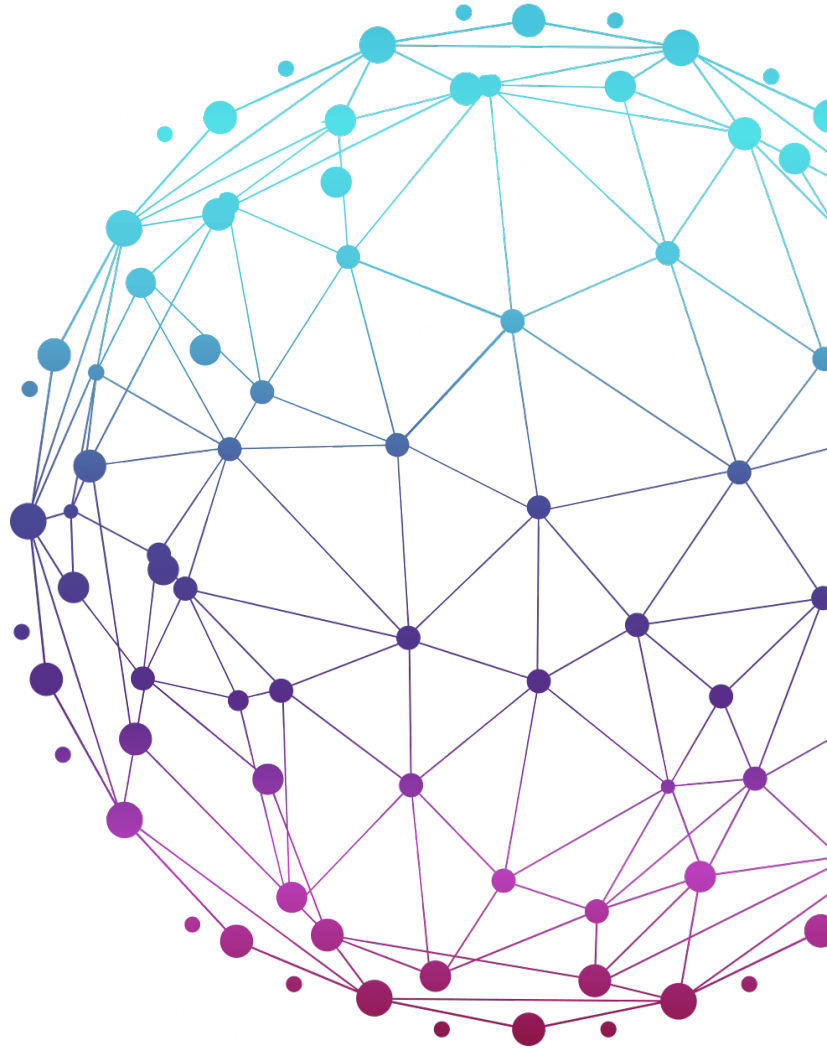
Чтобы быть частью системы, необязательно быть субъектом КИИ



Деятельность НКЦКИ

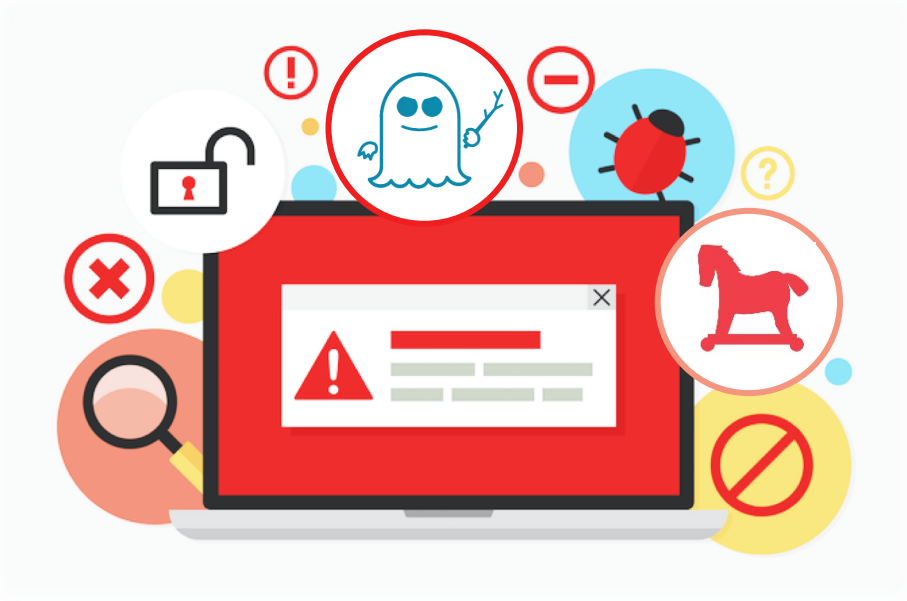
Организация информационного взаимодействия с созданием общего информационного пространства

Каждый участник может получить практическую помощь и внести свой вклад в общее дело



В ГосСОПКА организован обмен информацией

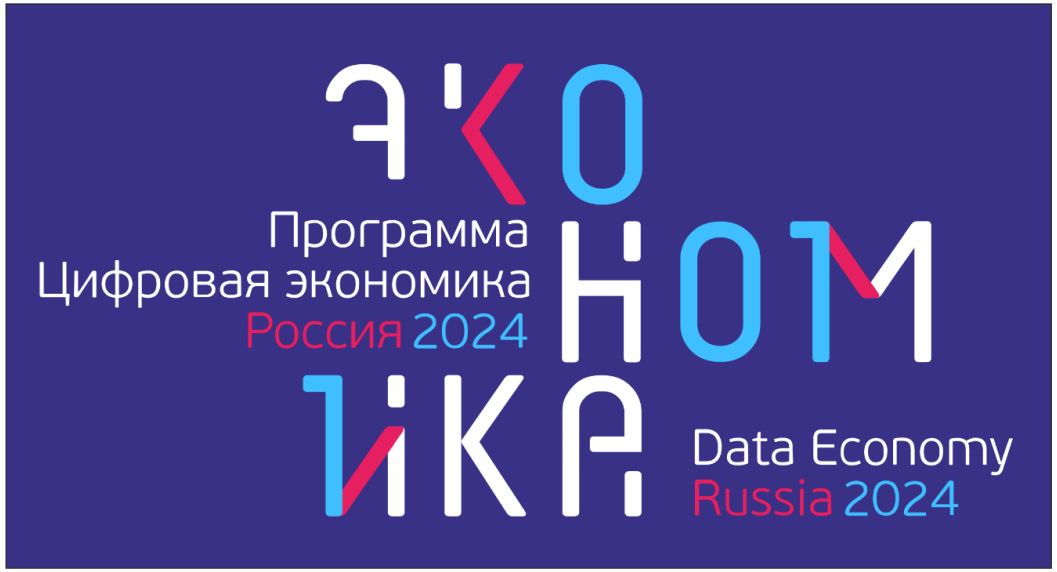
- Об источниках вредоносных воздействий
- О признаках компьютерных инцидентов
- Об угрозах
- Об уязвимостях ПО
- Индикаторами вредоносной активности (IOCs)

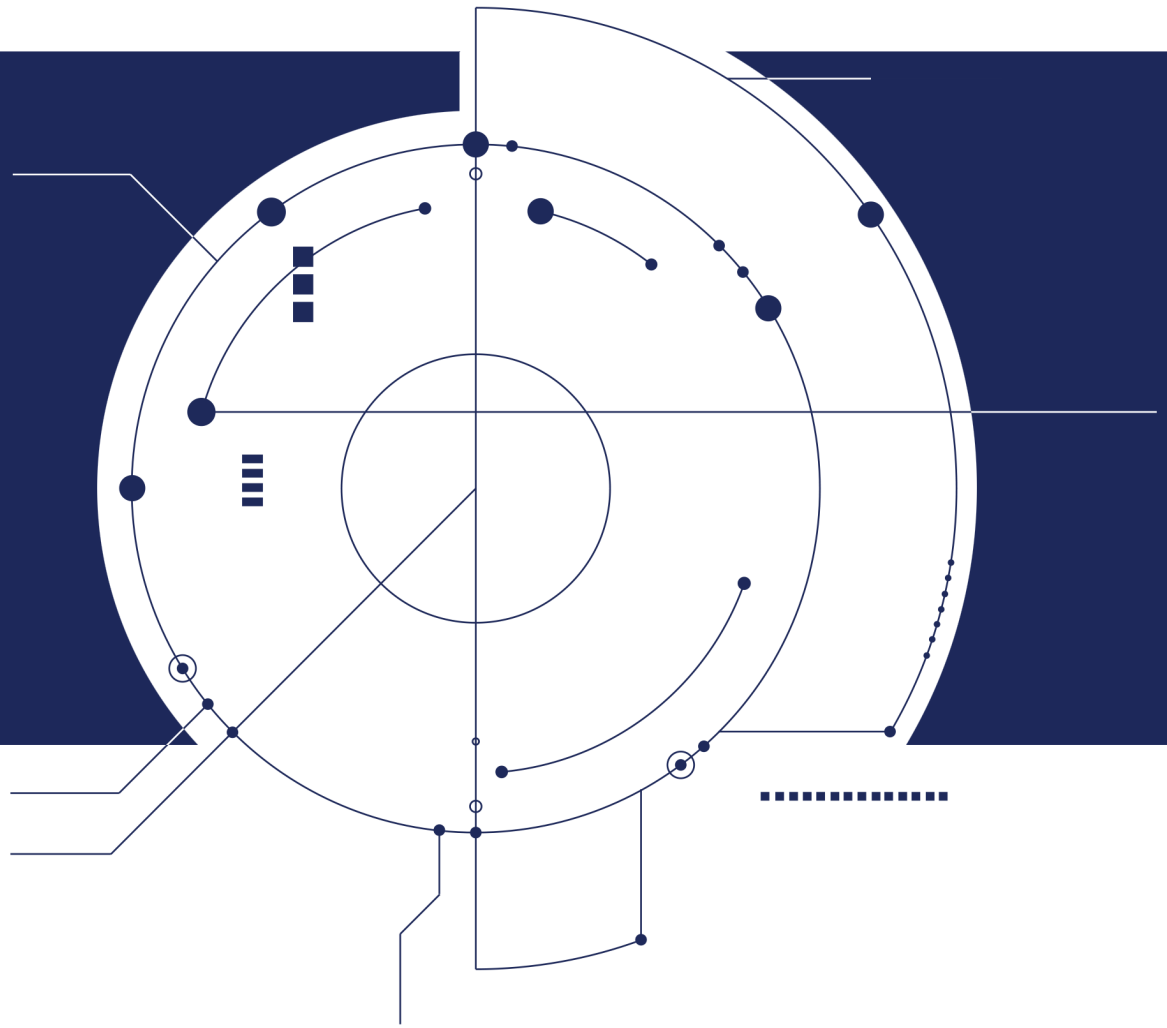


Созданы механизмы информационного взаимодействия

Система автоматизированного обмена сведениями о киберугрозах на базе технической инфраструктуры НКЦКИ

Создана в рамках реализации национальной программы «Цифровая экономика Российской Федерации»





Практические результаты

Выявление инцидентов

более **350** компьютерных инцидентов выявлено

Сведения о них и рекомендации по реагированию доведены до владельцев информационных ресурсов

Практическая помощь

около **700** раз специалисты НКЦКИ оказали содействие в реагировании на компьютерные инциденты

Практическая помощь

более **5,5 тысяч** вредоносных ресурсов заблокировано

Предотвращены масштабные компьютерные инциденты

Организован оперативный анализ информации

Выявлены критические уязвимости, эксплуатация которых могла привести к масштабным утечкам персональных данных граждан

Проинформированы производители уязвимых программных продуктов и пользователи

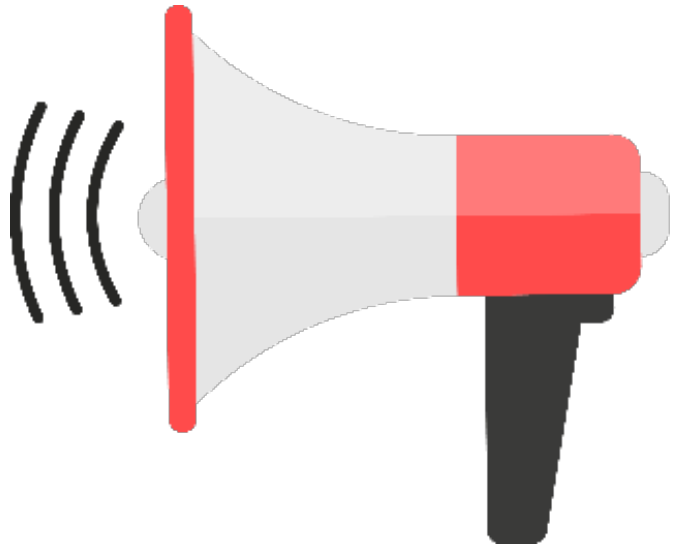
Совместно с ФСТЭК России выработаны меры по противодействию

Адресное информирование

около **180** бюллетеней об уязвимостях высокого и критического уровней опасности разослано участникам взаимодействия

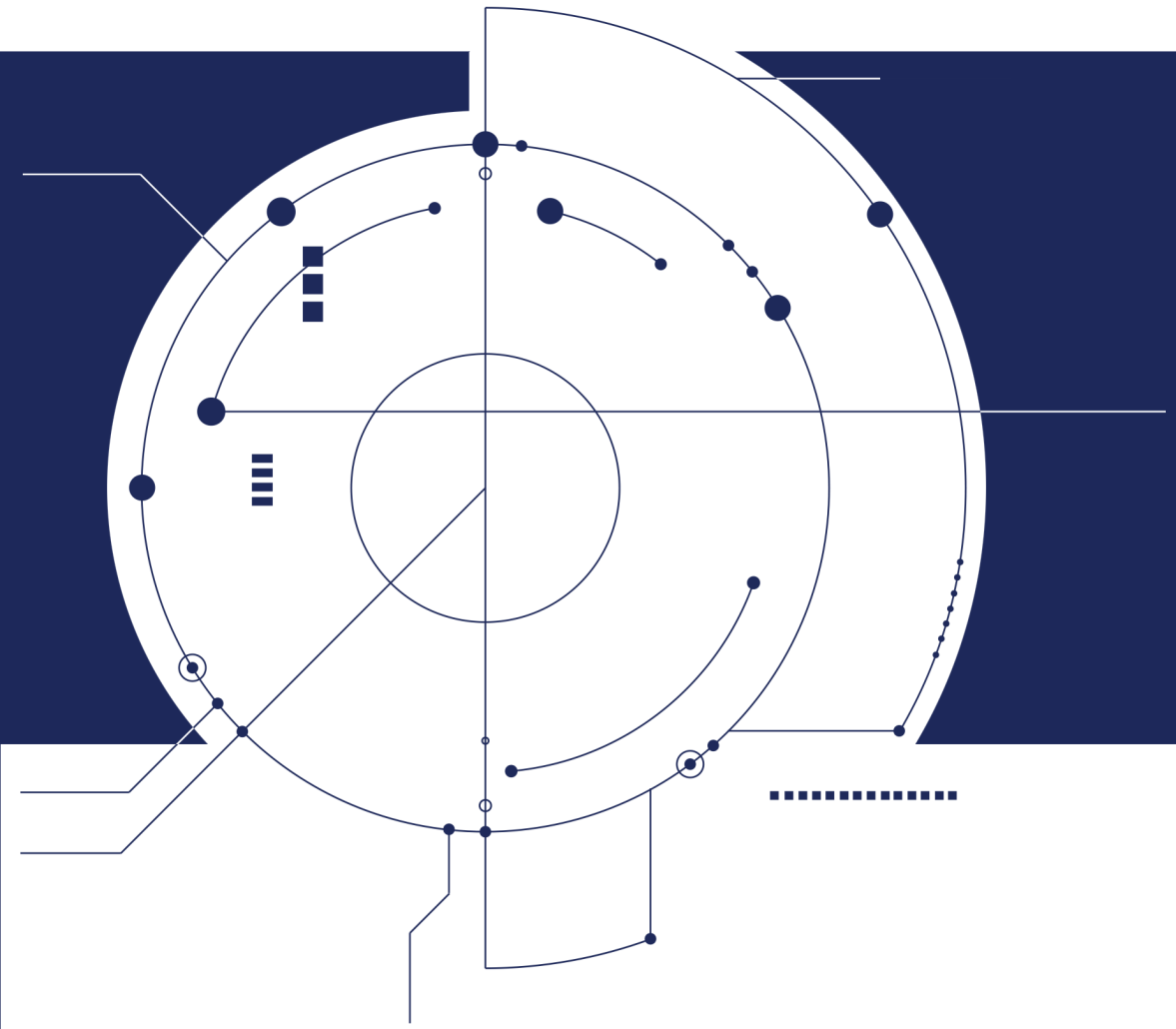
Масштабные кампании по информированию в 2019 году

- Об уязвимостях в ОС Windows
- Об уязвимостях в почтовом сервере Exim



Информационная безопасность требует внимания

Большое количество компьютерных инцидентов возникает из-за того, что владельцы информационных ресурсов не уделяют должного внимания вопросам информационной безопасности



ГосСОПКА для всех информационных ресурсов РФ!

Состав участников ГосСОПКА не ограничен

ГосСОПКА предназначена для всех информационных ресурсов Российской Федерации

Давайте работать сообща!

Спасибо за внимание!

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ