



Компания КОМПЛИТ

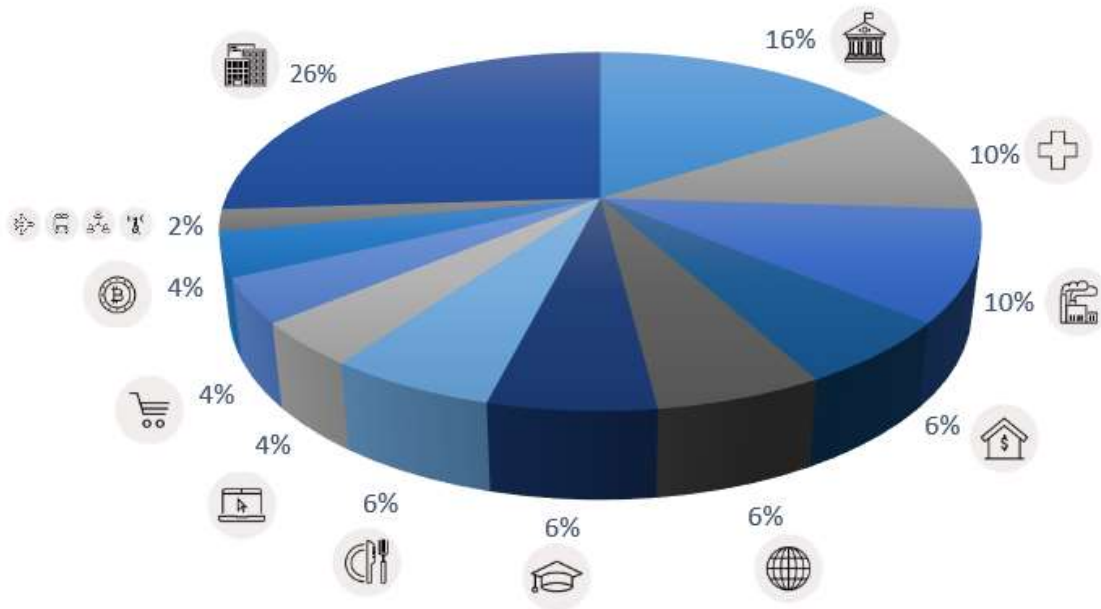
# Актуальные вопросы критической информационной инфраструктуры

Технический консультант  
Кузнецова Александра

[www.complete.ru](http://www.complete.ru)

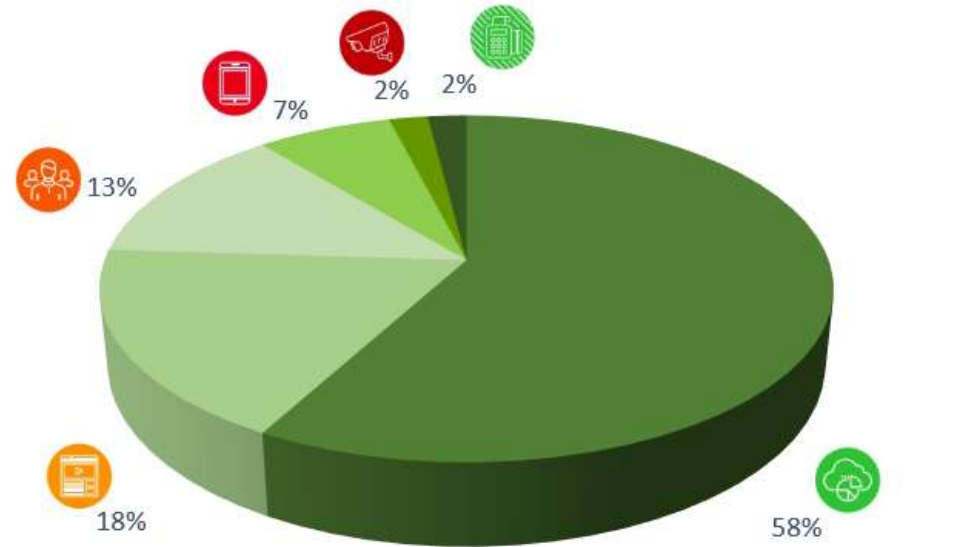
# Состояние киберугроз

## Атаки по отраслям



- Государственные учреждения
- Медицинские учреждения
- Промышленные компании
- Финансовая отрасль
- Онлайн-сервисы
- Наука и образование
- Сфера услуг
- IT-компании
- Торговля
- Блокчейн-проекты
- Другие
- Без привязки к отрасли

## Объекты атак



- Инфраструктура
- Веб-ресурсы
- Пользователи или сотрудники
- Мобильные устройства
- IoT
- Банкоматы и POS-терминалы

# Решение – ЕСТЬ!

Федеральный закон № 187-ФЗ от 26.07.2017 г.  
«О безопасности критической  
информационной инфраструктуры Российской  
Федерации»

Федеральный закон **регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры** Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.



# Кто? Что? Где?



## Объекты ККИИ

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные системы управления субъектов



## Сферы функционирования объектов КИИ

- здравоохранение
  - наука
  - транспорт
  - связь
  - энергетика
  - финансы
- топливно-энергетический комплекс
  - область атомной энергии
  - оборонная промышленность
- ракетно-космическая промышленность
- горнодобывающая промышленность
- металлургическая промышленность
  - химическая промышленность



## Субъекты КИИ

- Государственные органы
- Государственные учреждения
- Российские юридические лица
- Индивидуальные предприниматели

# КИИ В ВУЗе. Пример



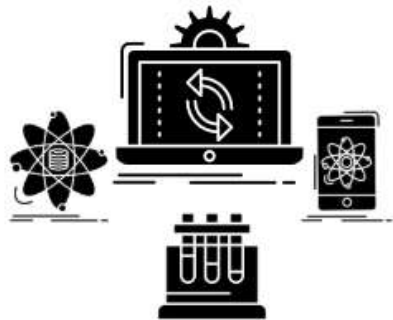
— ОКОПФ (верхний уровень)  
 ↳ ...  
 ↳ 75100 — Учреждения, созданные Российской Федерацией (уровень выше)  
 ↳ 75103 — Федеральные государственные бюджетные учреждения (текущий уровень)

Виды деятельности:

Основной (по коду ОКВЭД ред 2): 85.22 - Образование высшее  
 Дополнительные виды деятельности по ОКВЭД 2:

72.1	Научные исследования и разработки в области естественных и технических наук
72.19	Научные исследования и разработки в области естественных и технических наук прочие

Кафедра ядерной  
физики



Лаборатория и  
оборудование на  
радиоактивных  
элементах.  
Управление через ИС.

## Исходные данные

ВУЗ: Государственное учреждение

Вид деятельности: Высшее образование,  
научная деятельность

Имеет лабораторию под управлением  
информационной системы (ИС),  
функционирующей в области науки и  
находится на праве собственности ВУЗа

## ВЫВОД

ВУЗ - субъект КИИ

Лабораторная информационная  
система – объект КИИ

**ОБЯЗАТЕЛЬНОЕ выполнение требований  
ФЗ-187**

1. Категорирование объектов КИИ (ОКИИ)
2. Обеспечение безопасности значимых объектов КИИ (ЗОКИИ)
3. Присоединение к ГосСОПКА



# Порядок категорирования согласно ПП № 127 от 08.02.2018 г. (ред. от 13.04.2019 г.)



# Обеспечение безопасности значимых объектов КИИ (ЗОКИИ)

## Реализация основана на 5 шагах:

- Шаг 1. Формирование перечня применимых требований.
- Шаг 2. Разработка организационных и технических мер.
- Шаг 3. Внедрение организационных и технических мер по обеспечению безопасности.
- Шаг 4. Обеспечение безопасности во время эксплуатации.
- Шаг 5. Обеспечение безопасности при выводе из эксплуатации.

При выборе мер следует учитывать возможные угрозы на ЗОКИИ, а также соотношение категории значимости и требуемого класса СЗИ.

Категория объекта КИИ	Потенциал источника угроз, который следует рассматривать при выборе мер	Требуемый класс СЗИ
I категория	Высокий	Не ниже 4 класса
II категория	Базовый усиленный	Не ниже 5 класса
III категория	Базовый	Не ниже 6 класса





Основным назначением ГосСОПКА является **обеспечение защищенности информационных ресурсов** Российской Федерации **от компьютерных атак** и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

Главным центром ГосСОПКА является **Национальный координационный центр по компьютерным инцидентам** (далее - НКЦКИ).





## Федеральные законы

**Федеральный закон от 26.07.2017 № 193-ФЗ**  
«О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

**Федеральный закон от 26.07.2017 № 194-ФЗ**  
«О внесении изменений в УК и РФ и статью 151 Уголовно процессуального кодекса РФ в связи с принятием ФЗ «О безопасности КИИ РФ»



## Постановления Правительства РФ

**Постановление Правительства РФ от 08.02.2018 № 127 (ред. От 13.04.2019)**  
«Об утверждении Правил категорирования ОКИИ РФ, а также перечня показателей критериев значимости ОКИИ РФ»

**Постановление Правительства РФ от 17.02.2018 № 162** «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых ОКИИ РФ»

**Постановление Правительства РФ от 11.06.2018 № 808** «О внесении изменений в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК»

**Постановление Правительства РФ от 08.06.2019** «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых ОКИИ РФ»



## Приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК России)

**Приказ ФСТЭК России от 06.12.2017 № 227**  
«Об утверждении Порядка ведения реестра значимых ОКИИ РФ»

**Приказ ФСТЭК России от 11.12.2017 № 229**  
«Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых ОКИИ РФ»

**Приказ ФСТЭК России от 21.12.2017 № 235 ( ред. От 27.03.2019)** «Об утверждении Требований к созданию систем безопасности значимых ОКИИ РФ и обеспечению их функционирования»

**Приказ ФСТЭК России от 22.12.2017 № 236 (ред. От 21.03.2019)** «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

**Приказ ФСТЭК России от 25.12.2017 № 239(в ред. От 9.08.2018 , 26.03.2019)** «Об утверждении Требований по обеспечению безопасности значимых ОКИИ РФ»



## Приказы Федеральной службы безопасности (ФСБ России)

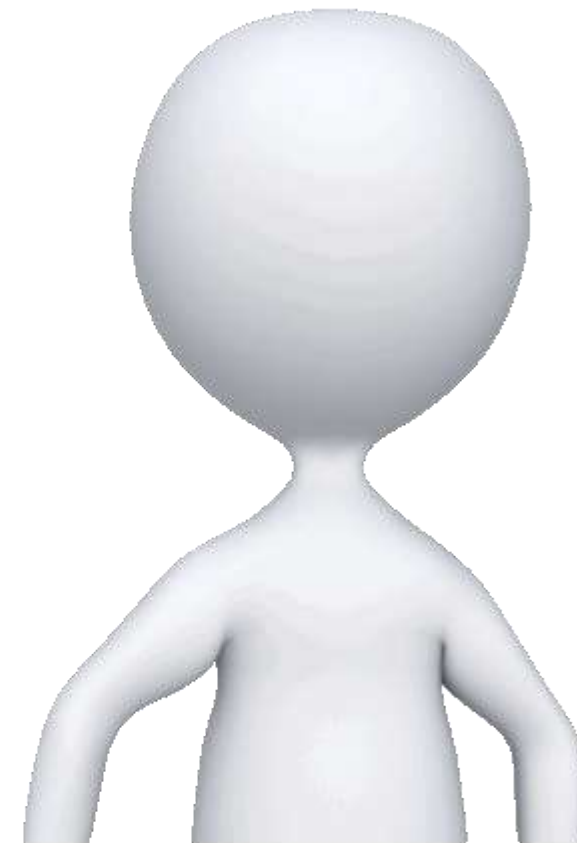
**Приказ ФСБ России от 24.07.2018 № 366** «О НКЦКИ»

**Приказ ФСБ России от 24.07.2018 № 367** «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

**Приказ ФСБ России от 24.07.2018 № 368** «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

**Приказ ФСБ России от 06.05.2019 № 196** «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

# Кто будет проверять?



# Надзор, контроль, запросы

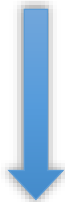


**ФСТЭК  
РОССИИ**

- Контроль и проверка правильности категорирования
- Ведение реестра значимых объектов КИИ
- Контроль соблюдения субъектами КИИ требований по обеспечению безопасности
- Плановые (раз в 3 года) и внеплановые выездные проверки



**ФСБ  
России**



**НКЦКИ**

- Оценка безопасности объектов КИИ
- Организация обмена информацией об инцидентах
- Установка средств контроля
- Запросы субъектам КИИ по вопросам обнаружения, предупреждения, ликвидации и реагирования на компьютерные инциденты
- Создание групп реагирования
- Привлечение экспертов для реагирования на компьютерные инциденты

Основание	Разъяснение	Мера
<p><b>"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 02.08.2019)</b>  <b>УК РФ Статья 274.1.</b>  <b>Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации</b>            (введена Федеральным законом от 26.07.2017 N 194-ФЗ)</p>	1.Создание, распространение и (или) использование ПО или иной компьютерной информации для неправомерного воздействия на КИИ:	принудительные работы <b>до 5 лет</b> / лишение свободы <b>до 5 лет</b> / штраф <b>до 1 млн руб</b>
	2.Неправомерный доступ к информации КИИ, если он повлѣк вред:	принудительные работы <b>до 5 лет</b> / лишение свободы <b>до 6 лет</b> / штраф <b>до 1 млн руб</b>
	3.Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ:	принудительные работы <b>до 5 лет</b> / лишение свободы <b>до 6 лет</b> / запрет занимать должности <b>до 3 лет</b>
	4.Деяния, предусмотренные частью первой, второй или третьей, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения:	лишение свободы <b>до 8 лет</b> / запрет занимать должности <b>до 3 лет</b>
	5.Деяния, предусмотренные частью первой, второй, третьей или четвертой, если они повлекли тяжкие последствия:	лишение свободы <b>до 10 лет</b> / запрет занимать должности <b>до 5 лет</b>

Спасибо за внимание!

ООО «Компания КОМПЛИТ»

Санкт-Петербург, ул. Яхтенная,  
д. 22, корп. 1, лит. А  
+7 (812) 740-3010

[info@complete.ru](mailto:info@complete.ru)

[www.complete.ru](http://www.complete.ru)