КСБИТ

# Анализ положений законодательства для владельцев КИИ

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

## ЗАДАЧА ЗАКОНА

При компьютерных атаках обеспечить устойчивое функционирование информационной инфраструктуры РФ, которые критически важны для экономики государства, т.е. объектов критической информационной инфраструктуры (КИИ).

Одним из главных принципов обеспечения безопасности является предотвращение компьютерных атак.

## В СЛУЧАЕ НЕИСПОЛНЕНИЯ ТРЕБОВАНИЙ

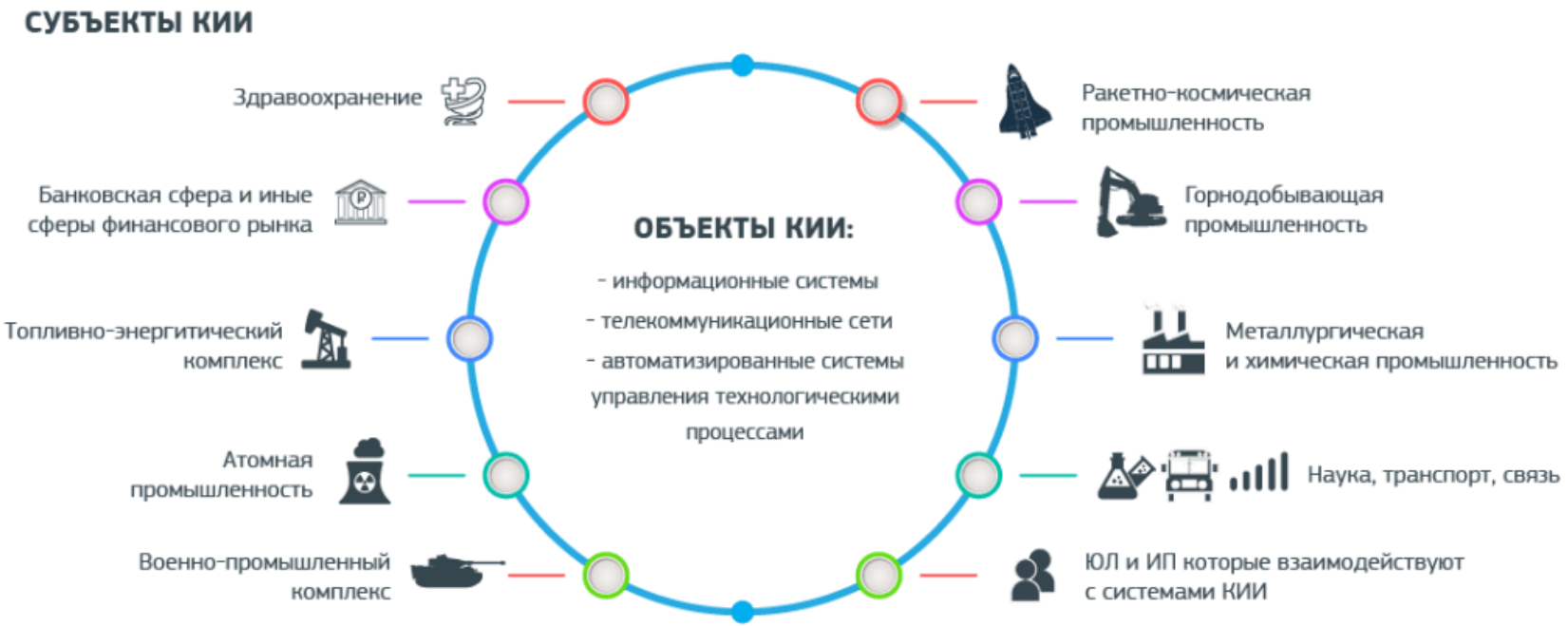
Согласно ст. 14 закона о безопасности КИИ: «Нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов влечет за собой **ответственность** в соответствии с законодательством Российской Федерации».

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

КСБИТ

# ОБЩАЯ ИНФОРМАЦИЯ

С 1 января 2018 года вступил в силу **Федеральный закон от 26.07.2017 г. № 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации», вместе с ним вступили в силу изменения в Уголовный кодекс РФ.



## О КАКОЙ ОТВЕТСТВЕННОСТИ ИДЕТ РЕЧЬ?

В уголовный кодекс Российской Федерации были внесены изменения принятием отдельного Федерального закона N 194-ФЗ от 26.07.2017 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

КСБИТ

# ЧАСТЬ 3, СТАТЬИ 274.1 УК РФ

***Нарушение правил***

эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи,

***если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, наказывается***

› *принудительными **работами на срок до пяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового,*

› *либо **лишением свободы на срок до шести лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.*

КСБИТ

# ЧАСТЬ 4, СТАТЬИ 274.1 УК РФ

***Деяния предусмотренные***

› частью первой (создание, распространение и (или) использование вредоносного ПО),

› второй (неправомерный доступ к охраняемой компьютерной информации)

› или третьей настоящей статьи, совершенные группой лиц по предварительному сговору, или организованной группой, или **лицом с использованием своего служебного положения**,

*наказываются **лишением свободы на срок от трех до восьми лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.*

КСБИТ

# ЧАСТЬ 5, СТАТЬИ 274.1 УК РФ

***Деяния предусмотренные***

- частью первой
- второй
- третьей или четвертой настоящей статьи,

***если они повлекли тяжкие последствия,***

*наказываются **лишением свободы на срок от пяти до десяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.*

КСБИТ

# АНАЛИЗ НОРМ И ИХ ПРИМЕНЕНИЕ

***Основные моменты***

***Предметом преступления*** для ч. 3, 4 и 5 ст. 274.1 УК РФ является электронно-вычислительная машина (ЭВМ):

- носитель информации,
- система ЭВМ,
- а также сети ЭВМ, которые имеют отношение к КИИ РФ.

***Объектом преступления*** выступают общественные отношения по обеспечению нормальной работы:

- функционированию ЭВМ,
- сети ЭВМ,
- системы ЭВМ, которые имеют отношение к КИИ РФ.

*Объективная сторона преступления может быть как **действием**, так и **бездействием**.*

*Нарушение правил эксплуатации заключается в несоблюдении правил работы с ЭВМ, сетями и другим оборудованием, нарушением должностных инструкций, а также нарушением правил обращения с охраняемой компьютерной информацией.*

**ПРИМЕР АКТИВНОГО ДЕЙСТВИЯ**

Системный администратор **учреждения здравоохранения** вычислял криптовалюту с использованием электрической сети этого учреждения.

**ПРИМЕР БЕЗДЕЙСТВИЯ**

Системный администратор не обновляет антивирусные базы.

Деяние, описанное в ч. 3 ст. 274.1, с объективной стороны характеризуется виной как в форме умысла, так и неосторожности. По аналогии со ст. 274 УК РФ лицо предвидит причинение вреда КИИ РФ в результате «нарушения им правил эксплуатации, но без достаточных к тому оснований самонадеянно рассчитывает на предотвращение последствий. Либо не предвидит указанных в законе последствий, хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть».

## О ВРЕДЕ И УЩЕРБЕ

Обязательным признаком для ч. 3 ст. 274.1 УК РФ является общественно - опасные последствия в виде причинения вреда критической информационной инфраструктуре Российской Федерации.

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

КСБИТ

# ОБ ОТВЕТСТВЕННОСТИ

***Без квалифицирующих признаков***

Ответственность за преступления, описанные ч. 3. ст. 274.1 УК РФ без квалифицирующих признаков, дифференцирована, и выбор остается за судом:

› *принудительными **работами на срок до пяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового,*

› *либо **лишением свободы на срок до шести лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.*

***С квалифицирующими признаками***

Часть 4 статьи 274.1 УК РФ гласит следующее: «Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения».

**В данной части квалифицирующими признаками будут:**

› *группой лиц по предварительному сговору или организованной группой;*

› *лицо с использованием своего служебного положения.*

## О КОМПАНИИ

Общество с ограниченной ответственностью “Комплексные системы безопасности информационных технологий” (“КСБИТ”) основано в 2018 году.

Специалисты компании обеспечивают комплексный подход при проектировании систем безопасности и встраивании средств защиты информации в существующие информационные системы, в том числе ГИС, ИСПДн, КИИ, АСУ ТП.

Наша команда состоит из профессионалов в области современных информационных технологий и имеет многолетний опыт реализации проектов по обеспечению безопасности информации различной степени сложности, что позволяет предлагать заказчикам наиболее эффективные решения, полностью соответствующие действующему законодательству.

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

КСБИТ

# ЗАЩИТА КИИ

**Компания ”КСБИТ”** – российская компания, поставщик и интегратор решений в сфере информационной безопасности, в том числе для госсектора и промышленных предприятий – оказывает услуги по выполнению требований 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" для организаций и предприятий причастных к критической информационной инфраструктуре РФ:

- определение объектов КИИ, принадлежность к субъектам КИИ;
- информирование ФСТЭК России об объектах КИИ, подлежащих категорированию;
- категорирование объектов КИИ, оформление необходимого набора документации;
- проектирование и внедрение систем защиты объектов КИИ;
- обеспечение непрерывной защиты систем КИИ и недопущение компьютерных атак на них;
- поддержка в вопросах информирования о произошедших с объектом КИИ инцидентах информационной безопасности;
- поддержка в вопросах реагирования и ликвидации последствий компьютерных инцидентов.


# ЭТАПЫ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ

**Компания "КСБИТ"** поможет реализовать этапы выполнения требований законодательства в области безопасности критической информационной инфраструктуры Российской Федерации:

I. Определение систем (объектов КИИ), обслуживающих критические процессы в организации/предприятии, с направлением перечня в ФСТЭК России.

II. Осуществление категорирования объектов КИИ с направлением результатов в ФСТЭК России.

III. Проектирование системы защиты КИИ, с учетом характеристик действующей инфраструктуры и актуальных угроз безопасности информации.

IV. Внедрение системы защиты значимых объектов КИИ по требованиям безопасности КИИ.

V. Поддержка и сопровождение системы обеспечения информационной безопасности. Выявление инцидентов и анализ уязвимостей объектов КИИ.

info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100

КСБИТ

# ЗАКЛЮЧЕНИЕ

В заключении можно отметить, что при сложности и несовершенстве законодательной базы и отсутствии судебной практики за совершение преступлений, описанных в ч. 3, 4, 5 статьи 274.1 УК РФ,

могут нести ответственность как *непосредственные исполнители*, так и *руководство юридических лиц или государственных органов*.

***Как можно снизить риски уголовной ответственности?***

В первую очередь – реализовать максимально возможную систему защиты информации на объекте КИИ. В любой непонятной ситуации обращаться к специалистам по технической защите информации или непосредственно в ФСТЭК России за разъяснениями. Поддерживать защиту в актуальном состоянии. Не забывать, что на объектах критической информационной инфраструктуры защите подлежит не только компьютерная система, но и иные объекты-носители защищаемых данных. Пользоваться только сертифицированными средствами защиты информации и актуальным ПО. Чтобы вовремя выявить и исправить возможные недостатки, нелишним будет изучать практику привлечения к ответственности по статьям 274 и 274.1 УК РФ, когда таковая появится.

# КОНТАКТЫ

КСБИТ

**ООО “КСБИТ”**
**214020, Россия, г. Смоленск, ул. Шевченко, д. 42**


**ОСТАЛИСЬ ВОПРОСЫ? СВЯЖИТЕСЬ С НАМИ!**

**info@ksbit.ru | www.ksbit.ru | +7 (4812) 610 100**