Заместитель руководителя Управления
ФСТЭК России по Сибирскому федеральному округу

БУЛГАКОВ Виктор Николаевич

Федеральный закон Российской Федерации №187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации».

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

вступил в силу с 1 января 2018 года

регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях её устойчивого функционирования при проведении в отношении её компьютерных атак

Основные понятия, используемые в 187-ФЗ:

Безопасность КИИ	состояние защищенности критической информационной инфраструктуры, обеспечивающее её устойчивое функционирование при проведении в отношении её компьютерных атак
Критическая информационная инфраструктура	объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов

Компьютерная атака	целенаправленное воздействие П и (или) ПА средств на объекты КИИ, сети электросвязи, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации
Компьютерная инцидент	факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушение безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки
Объекты КИИ	– информационные системы (ИС); – информационно-телекоммуникационные сети (ИТКС); – автоматизированные системы управления (АСУ)
Значимый объект КИИ	объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ

АСУ	комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами

Понятия, исходя из 149-ФЗ

(«Об информации, информационных технологиях и о защите информации»):

ИС	совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств
ИТКС	технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Субъекты КИИ

187-ФЗ

государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в сфере…

Определенные 187-ФЗ сферы деятельности:

Сфера здравоохранения

Банковская сфера и иные сферы финансового рынка

Сфера горнодобывающей промышленности

Сфера науки

Сфера энергетики и топливно-энергетического комплекса

Сфера металлургической промышленности

Сфера транспорта

Сфера атомной энергии

Сфера химической промышленности

Сфера связи

Сфера ракетно-космической промышленности

Сфера оборонной промышленности

Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры

Президент Российской Федерации

ОПРЕДЕЛЯЕТ:
-основные направления государственной политики;
-федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры (КИИ);
-федеральный орган исполнительной власти, уполномоченный в области функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА);
-порядок создания и задачи ГосСОПКА

Правительство Российской Федерации

УСТАНАВЛИВАЕТ:
-показатели критериев значимости объектов КИИ и их значения, порядок и сроки категорирования ;
-порядок осуществления государственного контроля;
-порядок подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов КИИ

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Указом Президента РФ от 25 ноября 2017 г. № 569 определена **ФСТЭК России**

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности КИИ;
2) утверждает порядок веления реестра значимых объектов КИИ;
3) утверждает форму направления сведений о результатах присвоения объектам КИИ одной из категорий значимости;
4) устанавливает требования по обеспечению безопасности значимых объектов КИИ;
5) осуществляет государственный контроль в области обеспечения безопасности значимых объектов КИИ, а также утверждает форму акта проверки

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Указом Президента РФ от 15 января 2013 г. №31с с учетом изменений, внесенных Указом от 22 декабря 2017 г. №620 определена **ФСБ России**

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности КИИ;
2) создает национальный координационный центр по компьютерным инцидентам;
3) координирует деятельность субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак;
4) организует и проводи оценку безопасности КИИ;
5) определяет перечень информации, представляемой в ГосСОПКУ, и порядок её представления;
6) утверждает порядок информирования о компьютерных инцидентах;
7) утверждает порядок обмена информацией о компьютерных инцидентах;
8) организует установку на значимых объектах КИИ средств ГосСОПКА;
9) устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак;
10) утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи

Федеральным законом «О связи» с учетом изменений, внесенных 193-ФЗ от 26 июля 2017 г. , определена **Минкомсвязь России**

-утверждает по согласованию с ФСБ России порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации Взаимодействия объектов критической информационной инфраструктуры

Центральный Банк Российской Федерации
(в соответствии в 187-ФЗ)

-согласовывает порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятии мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ в банковской сфере и в иных сферах финансового рынка

Права и обязанности субъектов критической информационной инфраструктуры

Права

1) получать от ФСТЭК России, информацию, необходимую для обеспечения безопасности значимых объектов КИИ, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой информации и уязвимостях программного обеспечения, оборудования и технологий, используемых на таких объектах;
2) в порядке, установленном ФСБ России, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;
3) при наличии согласия ФСБ России, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
4) разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ

Обязанности

всех субъектов КИИ

1) незамедлительно информировать ФСБ России о компьютерных инцидентах;
2) оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных атак;
3) в случае установки на объекте КИИ средств ГосСОПКА, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность

субъектов КИИ, имеющих значимые Объекты КИИ

1) Соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленных ФСТЭК России;
2) выполнять предписания должностных лиц ФСТЭК России об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные этими лицами в соответствии со своими компетенциями;
3) реагировать на компьютерные инциденты в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ;
4) Обеспечивать беспрепятственный доступ должностных лиц ФСТЭК России к значимым объектам КИИ при реализации полномочий по осуществлению государственного контроля

Изменения в законодательных актах в связи с принятием ФЗ-187

УК РФ → Введена ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

УПК РФ → Определена подследственность по уголовным делам за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации – ФСБ России

«Закон о гостайне» → Определено, что сведения о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак составляют государственную тайну

ФЗ-294 → Определено, что порядок установленный настоящим Федеральным законом, в части организации и проведения проверок, не применяется при осуществлении государственного контроля в области ОБ КИИ

ФЗ «О связи» → Определено, что:

-порядок подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов КИИ утверждается Правительством РФ;

-операторы связи в случае установки в сети электросвязи, используемой для организации взаимодействия объектов КИИ, средств, предназначенных для поиска признаков компьютерных атак обязаны обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств и их сохранность

СИСТЕМА НПА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИИ

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

Указы Президента РФ

Указ Президента РФ от 25.11.2017 г. № 569
«О внесении изменений в Положение о Федеральной службы по техническому и экспортному» (указ №1085, 2004 г.)

Указ Президента РФ от 02.03.2018 г. № 98
«О внесении изменений в Перечень сведений, отнесенных к государственной тайне» (Указ 1203, 1995 г.)

Постановления Правительства РФ

Постановление Правительства РФ
от 8.02.2018 г. № 127
«Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Постановление Правительства РФ
от 17.02.2018 № 162
«Об утверждении порядка осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

СИСТЕМА НПА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИИ

Приказы ФСТЭК России

от 06.12.2017 № 227 (зарегистрирован Минюстом России)
«Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»

от 11.12.2017 № 229 (зарегистрирован Минюстом России)
«Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

от 21.12.2017 № 235 (зарегистрирован Минюстом России)
«Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

от 22.12.2017 № 236 (зарегистрирован Минюстом России)
«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»

от 25.12.2017 № 239 (зарегистрирован Минюстом России)
«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Закон
«О государственной тайне»

Федеральный закон
«Об информации, информационных технологиях и о защите информации»

Федеральный закон
«О персональных данных»

Федеральный закон
«О безопасности критической информационной инфраструктуры Российской Федерации»

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну

Обеспечение безопасности значимых объектов, являющихся государственными информационными системами

Обеспечение безопасности значимых объектов, являющихся информационными системами персональных данных

Обеспечения безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

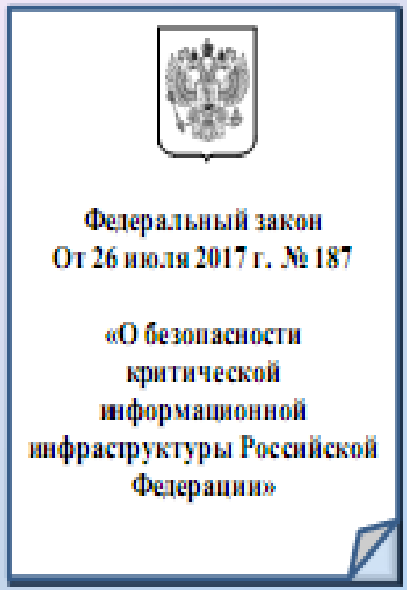
Законодательство РФ о государственной тайне

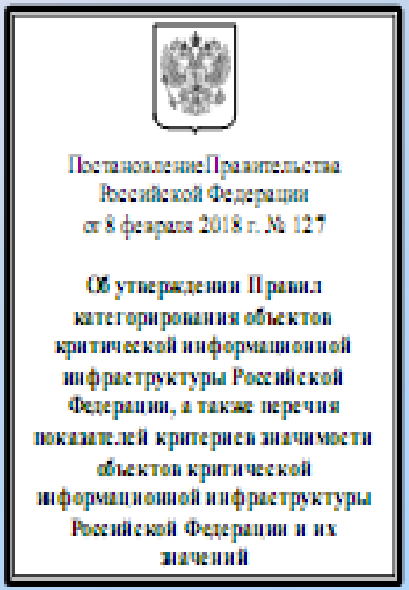
Приказ ФСТЭК России от 11 февраля 2013 г. № 17

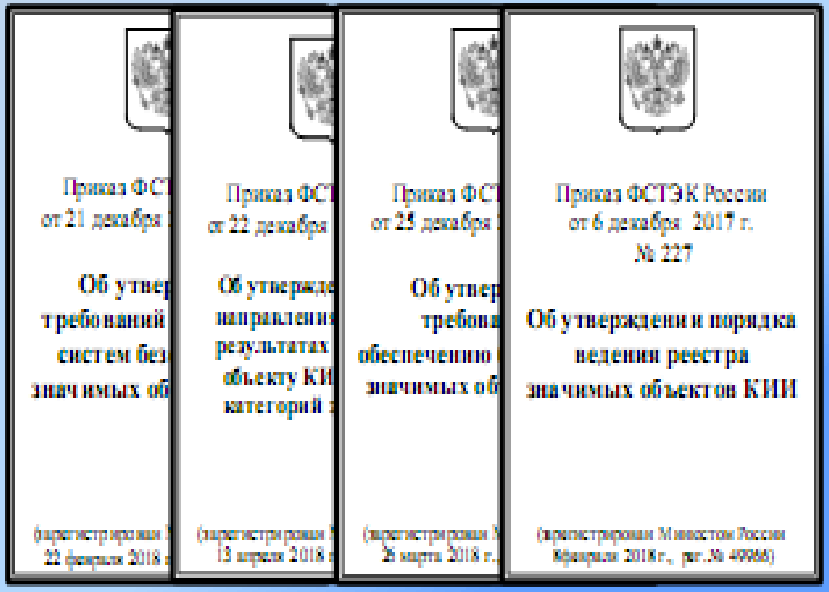
Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Нормативные правовые акты Минкомсвязи России

ПЕРВООЧЕРЕДНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ







- Категорирование объектов КИИ
- Создание систем безопасности значимых объектов
- Реализация требований по обеспечению безопасности значимых объектов
- Обеспечение взаимодействия с ГосСОПКА

СПАСИБО ЗА ВНИМАНИЕ!

630091, г.Новосибирск, Красный проспект, д.41
тел. 203-54-04