INFORMATION SECURITY LAB

Исполнение требований Законодательства по КИИ и ПД для системообразующих предприятий республики Башкортостан

Системообразующие организации Российской экономики

INFORMATION SECURITY LAB

Системообразующие предприятия (организации) Российской экономики – организации продукция или услуги которой важны для обеспечения жизни территории, функционирования определённой отрасли или социально-экономической системы страны или региона.

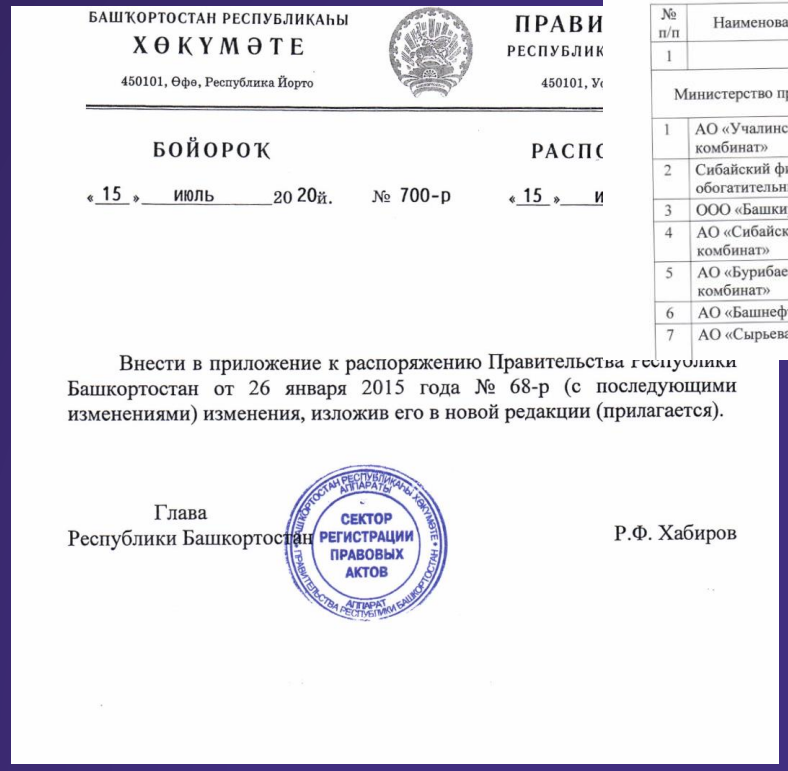
Системообразующие организации включаются в соответствующие **перечини** на основании отраслевых показателей по предложениям **федеральных органов исполнительной власти**, осуществляющих выработку государственной политики в соответствующих отраслях, а также **государственных корпораций**.

На уровне субъектов Федерации перечни системообразующих организаций формируются **региональными органами власти**.

Системообразующие организации в Башкортостане

Указ от 01 мая 2022 г. № 250 пункт 1

«и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):



БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ХӨКҮМӘТЕ
450101, Өфө, Республика Йорто

ПРАВИ
РЕСПУБЛИК
450101, У

БОЙОРОҠ

РАСПО

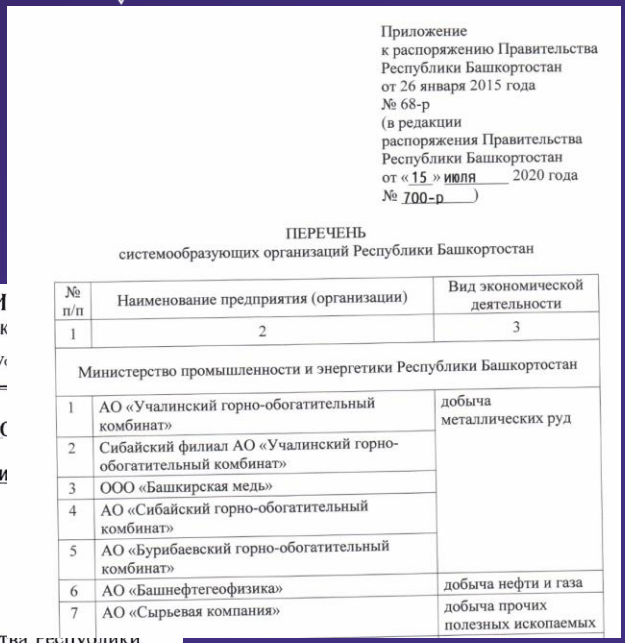
«15» июль 2020й. № 700-р «15» и

Внести в приложение к распоряжению Правительства Республики Башкортостан от 26 января 2015 года № 68-р (с последующими изменениями) изменения, изложив его в новой редакции (прилагается).

Глава
Республики Башкортостан

СЕКТОР РЕГИСТРАЦИИ ПРАВОВЫХ АКТОВ

Р.Ф. Хабиров



Приложение
к распоряжению Правительства
Республики Башкортостан
от 26 января 2015 года
№ 68-р
(в редакции
распоряжения Правительства
Республики Башкортостан
от «15» июля 2020 года
№ 700-р)

ПЕРЕЧЕНЬ
системообразующих организаций Республики Башкортостан

№ п/п	Наименование предприятия (организации)	Вид экономической деятельности
1	2	3
Министерство промышленности и энергетики Республики Башкортостан		
1	АО «Учалинский горно-обогатительный комбинат»	добыча металлических руд
2	Сибайский филиал АО «Учалинский горно-обогатительный комбинат»	
3	ООО «Башкирская медь»	
4	АО «Сибайский горно-обогатительный комбинат»	
5	АО «Бурибаевский горно-обогатительный комбинат»	
6	АО «Башнефтегеофизика»	добыча нефти и газа
7	АО «Сырьевая компания»	добыча прочих полезных ископаемых

Дополнительные меры защиты системообразующих предприятий с учетом Указа Президента РФ № 250

INFORMATION SECURITY LAB

Дополнительные мероприятия и обязанности в соответствии с Указом № 250:

- возложение **персональной** ответственности на руководителя организации за обеспечению информационной безопасности;
- возложение на заместителя руководителя организации полномочий по обеспечению информационной безопасности;
- создание отдельного структурного подразделения по обеспечению информационной безопасности организации, в том числе по организации защиты персональных данных и критической информационной инфраструктуры;
- постоянная оценка уровня защищенности организации;
- незамедлительная реализация организационных и технических мер, решения о необходимости осуществления которых принимают ФСБ России и ФСТЭК России;
- привлечение организаций аккредитованных ГосСОПКА к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Дополнительные меры защиты системообразующих предприятий с учетом Указа Президента РФ № 250

INFORMATION SECURITY LAB

Импортозамещение

В соответствии с положениями Указа Президента № 250 **с 1 января 2025 г.** органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств. Наряду с Указом Президента № 166, устанавливающим запрет на использование иностранного программного обеспечения, приказ № 250 является одной из финальных точек по достижению технологической независимости Российской Федерации.

Предположения и выводы

INFORMATION SECURITY LAB

Системообразующие компании синоним КИИ?

- Системообразующие компании – это КИИ * (как минимум стоит к этому готовиться)
- Отдельное и дополнительное внимание регуляторов по всем направления Законодательства
- Персональные данные – наше все, стоит приготовиться как минимум документально.
- Кадры, кадры и еще раз кадры.

Критическая информационная инфраструктура

Законодательство

С 1 января 2018 года вступил в силу Федеральный закон N 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации», определяющий автоматизированные системы управления, функционирующие в сфере в *сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности*, к объектам критической информационной инфраструктуры (далее – КИИ).

В соответствии с требованиями Федерального закона N 187-ФЗ субъектами КИИ должно быть осуществлено категорирование объектов КИИ и обеспечена их защита.

Критическая информационная инфраструктура

Что нужно сделать субъектам КИИ?

Субъекты КИИ должны выполнить следующие мероприятия:

- определить критические процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка;
- определить объекты КИИ которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- провести категорирование объектов КИИ - присвоение каждому из объектов КИИ одной из категорий значимости либо обосновывает принятие решения об отсутствии необходимости присвоения им одной из категорий значимости;
- отправить сведения о категорировании объектов КИИ во ФСТЭК России;
- реализовать организационные и технические мероприятий по защите значимых объектов КИИ;
- подключить значимые объекты КИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Критическая информационная инфраструктура

Ответственность за нарушение законодательства в области КИИ

КоАП РФ Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

ст. 13.12.1	Новое требование	Размеры штрафов
ч. 1	Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	для должностных лиц от 10 000 до 50 000 рублей для ЮЛ от 50 000 до 100 000 рублей.
ч. 2	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	для должностных лиц от 10 000 до 50 000 рублей для ЮЛ от 100 000 до 500 000 рублей.
ч. 3	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных	для должностных лиц от 20 000 до 50 000 рублей

Критическая информационная инфраструктура

Ответственность за нарушение законодательства в области КИИ

Федеральный закон о безопасности КИИ был принят вместе с законами-спутниками «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и «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».

В соответствии с изменениями Уголовный кодекс Российской Федерации дополнился статьей 274.1, которая повторяет статьи 272, 273 и 274, но в отношении объектов КИИ. Согласно пункту 3 статьи 274.1 УК РФ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ Российской Федерации, если оно повлекло причинение вреда КИИ 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.**

Критическая информационная инфраструктура

Что делать и как снизить риски?

- аудит процессов, анализ угроз и оценка значимости объектов КИИ;
- категорирование объектов КИИ;
- разработка необходимой организационно-распорядительной документации;
- моделирование угроз безопасности;
- проектирование системы защиты значимых объектов КИИ;
- установка и настройка средств защиты информации;
- мониторинг событий информационной безопасности значимых объектов КИИ и услуги корпоративного центра ГосСОПКА;
- Реализация положений Указа президента № 250 и ФЗ № 187.

Персональные данные

INFORMATION SECURITY LAB

Что нового в 2025 году?

ФЗ №420 от 30.11.2024

- Новые формы штрафов, значительное увеличение размеров ответственности.
- Новые составы ответственности за нарушения 152-ФЗ.
- Новые способы минимизации рисков.

ФЗ №421 от 30.11.2024

- Ответственность за получение данных без законных оснований (пользование слитыми данными).
- Ответственность за незаконный доступ к Персональным данным.
- Изменение структуры рисков для сотрудников по информационной безопасности.

Персональные данные

Что конкретно должен сделать оператор персональных данных?

1. Уведомить Роскомнадзор об обработке персональных данных.
2. Регламентировать процессы обработки и защиты персональных с учетом положений ФЗ-152 и подзаконных актов путем разработки и утверждения внутренней организационно-распорядительной документации.
3. Обеспечить защиту персональных данных хранящихся на материальных носителях.
4. Реализовать защиту персональных данных, обрабатываемых в информационных системах с использованием организационных и технических мер защиты в соответствии с требованиям ФСТЭК России и ФСБ России.

Персональные данные

Подробнее про 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

- Увеличение всех размеров ответственности вплоть до оборотного штрафа (1-3% от всех доходов).
- 9 новых составов правонарушения.
- Изменение подхода законодателя к нарушениям в сфере ПДн, смена значимости обеспечения информационной безопасности для организации.
- Увеличение ответственности за неуведомление РКН о начале обработки данных.
- Повышение важности внутреннего расследования инцидентов ИБ.

Персональные данные

INFORMATION SECURITY LAB

Подробнее про 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»

- Статья 272.1 – ответственность за использование ПДн, полученных незаконным путем, включая сбор без согласия субъекта или за рамками такого согласия.
- 6 составов, ответственность до 10 лет лишения свободы.
- Нарушение неприкосновенности частной жизни теперь отделено от неосновательного сбора персональных данных.

Персональные данные

INFORMATION SECURITY LAB

Когда изменения вступят в силу?

С **11.12.2024** года – Уголовная ответственность за незаконное использование ПДн

С **30.05.2025** года:
Оборотные штрафы за допущение утечки
Штрафы за отсутствие уведомления РКН
Увеличение штрафов за нарушение условий обработки

До **30.05.2025** года необходимо провести комплексную проверку документов, устанавливающих порядок взаимодействия с персональными данными, направить уведомления о намерении осуществлять обработку персональных данных, а также провести аудит средств защиты информации и процессов их обработки.

Персональные данные

Как изменятся штрафы?

INFORMATION SECURITY LAB

Нарушение	До 29.05.2025	С 30.05.2025
Нарушение цели и объема обработки ПДн (ст. 13.11 КоАП ч.1)	Для граждан от 2 000 до 6 000 рублей Для должностных лиц от 10 000 до 20 000 рублей Для ЮЛ от 60 000 до 100 000 рублей.	Для граждан от 10 000 до 15 000 рублей Для должностных лиц от 50 000 до 100 000 рублей Для ЮЛ от 150 000 до 300 000 рублей.
Повторное нарушение цели и объема обработки (ст. 13.11 КоАП ч.1.1)	Для граждан от 4 000 до 12 000 Для должностных лиц от 20 000 до 50 000 рублей Для ИП от 50 000 до 100 000 рублей Для ЮЛ от 100 000 до 300 000 рублей.	Для граждан от 15 000 до 30 000 рублей Для должностных лиц от 100 000 до 200 000 рублей Для ЮЛ от 300000 до 500 000 рублей.
Не уведомление РКН об намерении обрабатывать персональные данные (ст. 19.7 КоАП)	Для ЮЛ 5000 рублей	Для граждан от 5000 до 10000 рублей Для должностных лиц от 30000 до 5 000 рублей. Для ЮЛ от 100000 до 300000 рублей.
Не уведомление РКН об утечке (ст. 19.7 КоАП)	Для ЮЛ 5 000 рублей	Для граждан от 50 000 до 100 000 рублей Для должностных от 400 000 до 800 000 рублей Для ЮЛ от 1 млн до 3 млн рублей.

Персональные данные
Какие новые штрафы появятся?

INFORMATION SECURITY LAB

ст. 13.11 КоАП	Новое требование	Размеры штрафов
ч. 10	Неуведомление РКН об обработке персональных данных (обязанность оператора по ст. 22 152-ФЗ)	для граждан от 5 000 до 10 000 рублей для должностных лиц от 30 000 до 50 000 рублей для ЮЛ от 100 000 до 300 000 рублей.
ч. 11	Неуведомление РКН об утечке (обязанность оператора по ч.3.1 ст.21 152-ФЗ)	для граждан от 50 000 до 100 000 рублей для должностных лиц от 400 000 до 800 000 рублей для ЮЛ от 1 000 000 до 3 000 000 рублей.
ч. 12	Утечка персональных данных от 1 000 до 10 000 субъектов, и/или от 10 000 до 100 000 идентификаторов.	для граждан от 100 000 до 200 000 рублей для должностных лиц от 200 000 до 400 000 рублей для ЮЛ от 3 000 000 до 5 000 000 рублей.
ч. 13	Утечка персональных данных от 10 000 до 100 000 субъектов, и/или от 100 000 до 1 000 000 идентификаторов.	для граждан от 200 000 до 300 000 рублей для должностных лиц от 300 000 до 500 000 рублей для ЮЛ от 5 000 000 до 10 000 000 рублей.
ч. 14	Утечка персональных данных более 100 000 субъектов, и/или более 1 000 000 идентификаторов.	для граждан от 300 000 до 400 000 рублей для должностных лиц от 400 000 до 600 000 рублей для ЮЛ от 10 000 000 до 15 000 000 рублей.
ч. 15	Если оператор уже подвергнут административному наказанию по ч.12-14 и вновь происходит утечка (по ч.12-14 и ч.16-18).	для граждан от 400 000 до 600 000 рублей для должностных лиц от 800 000 до 1 000 000 рублей для ЮЛ от 1% до 3% выручки за год, но не менее 20 000 000 и не более 500 000 000 рублей.
ч. 16	Утечка специальных категорий персональных данных.	для граждан от 300 000 до 400 000 рублей для должностных лиц от 1 000 000 до 1 300 000 рублей для ЮЛ от 10 000 000 до 15 000 000 рублей.
ч. 17	Утечка биометрических персональных данных.	для граждан от 400 000 до 500 000 рублей для должностных лиц от 1 300 000 до 1 500 000 рублей для ЮЛ от 15 000 000 до 20 000 000 рублей.
ч. 18	Если оператор уже подвергнут административному наказанию по ч.12 - 17 и происходит утечка специальных	для граждан от 500 000 до 800 000 рублей для должностных лиц от 1 500 000 до 2 000 000 рублей

Персональные данные

INFORMATION SECURITY LAB

Что делать и как снизить риски?

- аудит процессов, правовых оснований и условий обработки персональных данных;
- разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты персональных данных;
- моделирование угроз безопасности;
- проектирование системы защиты информационных систем персональных данных;
- установка и настройка средств защиты информации;
- аттестация информационных система персональных данных по требованиям безопасности.

Общество с ограниченной ответственностью «ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

INFORMATION SECURITY LAB

Предлагаем корпоративные решения для кибербезопасности, которые помогут вам добиться успеха в условиях неопределенности.

Мы знаем, как построить защиту эффективно, соразмерно и адаптировать под ваши бизнес-процессы.

info@islg.ru

8-495-723-72-75

@information_security_lab

www.islg.ru