Сергей Акимов
заместитель генерального директора
по спецпроектам и стандартизации

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

Обзор нормативной базы. Изменения и дополнения

Участники:

- ✓ Президент
- ✓ Правительство
- ✓ ФСБ России
- ✓ ФСТЭК России
- ✓ Минцифры (в частности Роскомнадзор)
- ✓ Центральный банк
- ✓ Отраслевые министерства и ведомства
- ✓ Технические комитеты

(в частности ТК №26, ТК №362, ТК №126, **ТК №167«ПАК для КИИ и ПО для них»**)

Направления деятельности:

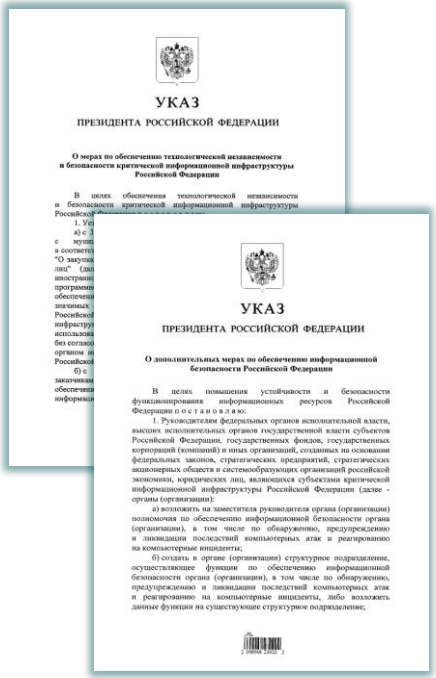
- ✓ КИИ
- ✓ ГосСОПКА
- ✓ ПДн
- ✓ ГИС
- ✓ Защита ГТ и КИ
- ✓ Лицензирование и сертификация
- ✓ Ведение Реестров

(Российского ПО, ЕРРРП, ТОРП)

Указы Президента. Технологическая независимость и усиление ИБ

1) О мерах по обеспечению технологической независимости и безопасности КИИ РФ (Указ №166 от 30 марта 2022 г.)

- **с 31 марта закупка иностранного ПО для ЗО КИИ только по согласованию** с уполномоченным ФОИВом
- **с 1 января 2025 г. запрещается использовать иностранное ПО на ЗО КИИ**
- преимущественное **применение ДОВЕРЕННЫХ ПАК на ЗО КИИ**
- **запрет на закупки** из недружественных стран


УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ
О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации
УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ
О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

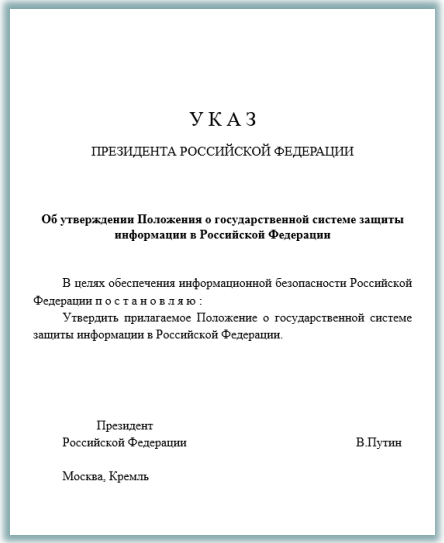
2) О дополнительных мерах по обеспечению ИБ РФ (Указ №250 от 1 мая 2022 г.)

- **вводится персональная ответственность руководителей за состояние ИБ**
- для ряда предприятий **вводится должность заместителя руководителя по ИБ**
- **обязательно создание структурного подразделения**, осуществляющего функции по обеспечению ИБ
- **обеспечение незамедлительной реализации орг. и тех. мер**, решение об осуществлении которых принимаются **ФСБ и ФСТЭК России**
- проведение дополнительных мероприятий по линии функционирования НКЦКИ, ГосСОПКИ

Об утверждении Положения о гос.системе защиты информации в РФ

Среди основных направлений деятельности ГСЗИ:

- Проведение единой политики в области ЗИ
- Координация деятельности участников системы на уровнях от объектового до федерального
- Прогнозирование, выявление и оценка угроз безопасности информации
- Обеспечение целостности и конфиденциальности обрабатываемой информации
- Создание и внедрение способов и методов ЗИ
- Контроль обеспечения ЗИ
- Подготовка кадров в области ЗИ



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Положения о государственной системе защиты информации в Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю :

Утвердить прилагаемое Положение о государственной системе защиты информации в Российской Федерации.

Президент
Российской Федерации В.Путин

Москва, Кремль

Исполнение Указа № 250. ФСБ России

Указ «О дополнительных мерах по обеспечению ИБ РФ»

Проект приказа ФСБ России «Об утверждении Порядка осуществления мониторинга защищенности информационных ресурсов…»

- ✓ мониторинг защищенности **будет осуществляться 8 Центром ФСБ России и территориальными органами безопасности**
- ✓ **оценка защищенности информационных ресурсов должна будет осуществляться на основании ежегодного плана**
- ✓ для оценки защищенности информационных ресурсов **потребуется подключение ПАКов органов безопасности к информационным ресурсам органов (организаций)**

Приказ ФСБ России от 01.11.2022г. №543 «Об определении переходного периода…»

- ✓ определен **переходный период (3 года) в** течение которого **допускается осуществлять мероприятия по обнаружению и реагированию на основании заключенных с НКЦКИ соглашений** о сотрудничестве в данной области
- ✓ **по истечении переходного периода допускается привлечение только аккредитованных центров гос.системы ОПЛПКА**

Исполнение Указа № 250. Правительство, ФСБ России, Росстандарт

Указ «О дополнительных мерах по обеспечению ИБ РФ»

ПРАВИТЕЛЬСТВО:

- ✓ типовое **положение о заместителе руководителя органа (организации)**, ответственном за обеспечение ИБ
- ✓ типовое **положение о структурном подразделении в органе (организации)**, обеспечивающем ИБ

РОССТАНДАРТ, ФСБ России:

- ✓ ГОСТ Р 59709-2022 «ЗИ. **Термины и определения**»
- ✓ ГОСТ Р 59710-2022 «ЗИ. **Общие положения**»
- ✓ ГОСТ Р 59711-2022 «ЗИ. **Организация деятельности по управлению компьютерными инцидентами**»
- ✓ ГОСТ Р 59712-2022 «ЗИ. **Руководство по реагированию на компьютерные инциденты**»

Исполнение Указа № 166. Доверенные ПАКи

Указ «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»

Обеспечить создание и организацию деятельности НПО, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных ПАК для КИИ

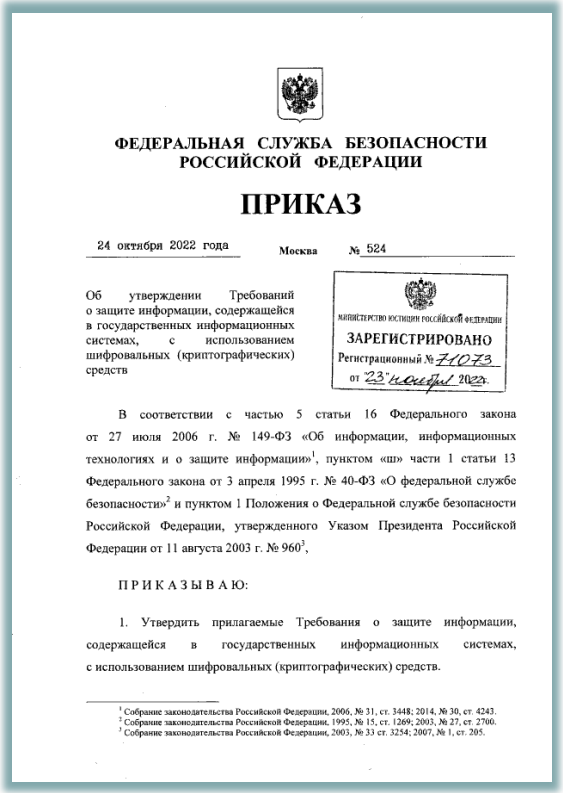
Распоряжение Правительства РФ
от 29 марта 2023 г. N757-р
«Об определении АО «НПО "Критические информационные системы»
НПО, специализирующимся на разработке, производстве…

Приказ Росстандарта
от 9 декабря 2022 г. №3107
«Об организации деятельности ТК по стандартизации «ПАК для КИИ и ПО для них»
Возложить функции по ведению дел секретариата ТК на АО «НПО «Критические информационные системы»

ФСБ России.
Защита информации в ГИС

Приказ ФСБ России от 24 октября 2022 г. №524
«Об утверждении Требований о защите информации, содержащейся в ГИС, с использованием шифровальных (криптографических) средств»

- **распространяется на ГИС не содержащие сведений, составляющих ГТ**
- необходимость использования СКЗИ подлежит обоснованию в МУ, которая согласуется с ФСБ России
- **вводятся Уровни значимости информации** в ГИС
- **допускается использование только сертифицированных в системе ФСБ России СКЗИ**
- **класс СКЗИ, используемых в ГИС, определяется для каждого сегмента ГИС,** либо для ГИС в целом



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 октября 2022 года Москва № 524

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71073
от 23 ноября 2022

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], пунктом «ш» части 1 статьи 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»[2] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[3],

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств.

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2014, № 30, ст. 4243.
[2] Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2003, № 27, ст. 2700.
[3] Собрание законодательства Российской Федерации, 2003, № 33 ст. 3254; 2007, № 1, ст. 205.

Правила определения минимально допустимого класса СКЗИ

Уровень значимости информации (УЗ)	Масштаб ГИС (сегмента ГИС)		
	На всей территории РФ или в пределах двух и более субъектов РФ	В пределах одного субъекта РФ	В пределах объекта (объектов) одного гос. органа, муниципального образования и (или) организации
Высокий УЗ	**КВ**	КС3	КС2
Средний УЗ	КС3	КС3	КС1
Низкий УЗ	КС2	КС1	КС1

ФСБ России. Защита сведений

Приказ ФСБ России от 4 ноября 2022 г. №547

«Об утверждении Перечня сведений в области военной, военно-технической деятельности РФ, которые при их получении иностранными источниками могут быть использованы против безопасности РФ»

- **сведения об использовании технологий криптографической ЗИ, квантовых технологий,** при разработке и производстве новых (перспективных) образцов вооружения, военной и специальной техники
- **сведения о составе и организации работы ГИС и КИИ,** исходных текстах и дистрибутивах ПО, применяемого в работе ГИС и объектов КИИ, технической документации (ТЗ, МУ и МН), настройках СЗИ
- **результатах анализа защищенности и реагирования на компьютерные инциденты ИБ** ГИС и КИИ
- **сведения о проведении закупок в части ПО и ПА средств** для нужд предприятий ОПК

Вопросы разработки СКЗИ. Новые/старые ГОСТы

1) Принято решение **отложить дату запрета на использование ГОСТ 28147-89 до** 1 июня 2024 г.
2) ТЗ на разработку СКЗИ должны содержать поддержку новых ГОСТ, **использование старых ГОСТ возможно для обеспечения совместимости работы с действующими ИС**
3) 8 Центр готов принимать изделия на **КТИ без реализации в СКЗИ новых ГОСТ**
4) Возможно **продление срока действия заключения и сертификата,** ограниченных 1 июня 2024 г.

Сертификаты на ViPNet

№ п/п	Наименование изделия	Заканчивается 01.06.2024	Возможность продления сертификата
1.	**ПАК ViPNet L2-10G**	№СФ/124-4266	до **04.05.2027**
2.	**ПАК ViPNet QSS Server**	№СФ/124-4371	до **30.09.2027**
3.	**ПАК ViPNet QSS Point**	№СФ/124-4372	до **30.09.2027**
4.	**ПАК ViPNet PKI Service** (АП HSM2000Q2)	№СФ/124-4328	до **31.10.2024**
5.	**ПАК ViPNet HSM** (исполнение 6)	№СФ/124-4330	до **31.10.2024**
6.	**ПАК ViPNet Coordinator IG 4** (АП IG10 I1, IG10 I2, IG100 I1)	№СФ/124-4247	до **19.05.2027**
7.	**ПАК ViPNet Coordinator HW 4** (HW50 A, HW50 B, HW100, HW1000, HW1000C, HW1000 D, HW2000, HW5000)	№СФ/124-4156	до **29.10.2026**
8.	**ПАК ViPNet Coordinator HW 4** (ViPNet Coordinator VA)	№СФ/124-4138	до **29.10.2026**
9.	**ПАК ViPNet Coordinator HW 4** (АП HW2000 Q5)	№СФ/124-4449	до **30.12.2027**
10.	**ПАК ViPNet Coordinator KB 4** (АП KB1000 Q8)	№СФ/124-4167	до **18.11.2026**
11.	**ПАК ViPNet Coordinator KB 4** (АП KB1000 Q7)	№СФ/124-4216	до **31.12.2025**
12.	**ПАК ViPNet Coordinator KB 4** (B100, KB1000, KB2000, KB5000)	№СФ/124-4215	до **31.12.2025**
13.	**ПК ViPNet Client 4U for Android**	№СФ/114-4380	до **06.10.2027**

ФСТЭК России. Повышение защищенности информационной инфраструктуры.

Приказы/указания 2022-2023 гг.

О мерах по повышению защищенности
(два Указания ФСТЭК России от 24.04.2022г и от 28.03.2023г.)

- Блокировка или ограничение доступа извне к сетевым службам
- Усиление требований по парольной защите
- Использованием двухфакторной аутентификация и защищенных каналов передачи данных при удаленном доступе
- Исключение удаленной технической поддержки для потребителей либо с использованием VPN-сетей
- Отказ от использования незащищенных протоколов управления

Об отзыве сертификатов
(6 приказов)

- **в связи с невыполнением требований доверия - 37 СЗИ**
- **в связи с попаданием под перечень иностранных государств и территорий, совершающих недружественные действия в отношении РФ - 40 СЗИ**

ФСТЭК России. Совершенствование системы защиты информации

Изменение процедур проведения работ

- **Изменения в Положение о системе сертификации** (**Приказ ФСТЭК России № 172, Указания ФСТЭК России об особенностях сертификации СЗИ от 21.03.2022 г. и 17.01.2023 г.**):
  - **Сокращение сроков** рассмотрения документов по сертификации СЗИ и сроков проведения отдельных работ
  - **Возможность проведение дополнительных испытаний разработчиком** СЗИ при внесении изменений
  - **Упрощение порядка** реализации процедуры **внесения изменений**
- **Совершенствование безопасной разработки программного обеспечения**
- **Совершенствование процедур аккредитации**
- **Изменения в требования доверия**

Изменение требований к СЗИ

- **Требования по безопасности информации к средствам контейнеризации**
  (утверждены Приказом ФСТЭК России от 4 июля 2022 г. № 118)
- **Требования по безопасности информации к средствам виртуализации**
  (утверждены Приказом ФСТЭК России от 2 октября 2022 г. № 187)
- **Требования по безопасности информации к многофункциональным МЭ уровня сети**
  (утверждены Приказом ФСТЭК России от 7 марта 2023 г. №44)
- **Требования по безопасности информации к системам управления базами данных** (готовится проект)
- **Требования по безопасности информации к межсетевым экранам** (готовится проект)
- **Требования по безопасности информации к системам обнаружения вторжений** (готовится проект)

Изменения в требования доверия

Приказ ФСТЭК России от 18 апреля 2022 г. №68 (зарегистрирован Минюстом России 20 июля 2022 г. №69318)

Применение отечественных аппаратных платформ СЗИ (с 5 уровня доверия) и СВТ, являющихся средой функционирования СЗИ (с 3 уровня доверия)	~~С 01 января 2022~~ → С 01 января 2024
Применение отечественных процессоров, микросхем, элементов памяти, сетевых карты, графических адаптеров СЗИ (с 4 уровня доверия)	~~С 01 января 2024~~ → С 01 января 2026
Применение отечественных процессоров, микросхем, элементов памяти, сетевых карты, графических адаптеров СВТ, являющихся средой функционирования СЗИ (с 2 уровня доверия)	~~С 01 января 2026~~ → С 01 января 2030

Требования к многофункциональным МЭ

Многофункциональный межсетевой экран уровня сети – программно-аппаратное средство, реализующее контроль за информацией и обеспечивающее защиту информационной (автоматизированной) системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования

Предъявляются требования к:

- ✓ Обнаружению и блокированию компьютерных атак
- ✓ Обнаружению и блокированию вредоносного ПО
- ✓ Доверенной загрузке МЭ (с применением сертифицированного СДЗ)
- ✓ Производительности МЭ (должны быть зафиксированы сведения о пропускной способности, подтвержденные методикой)
- ✓ Применению сертифицированных СКЗИ
- ✓ Аппаратной фильтрации ……

Фильтрация трафика на основе:

- ✓ GeoIP
- ✓ Двоичных флагов управления сетевым соединением
- ✓ Сигнатур приложений
- ✓ Типов файлов, информационных объектов, контента
- ✓ DPI
- ✓ ……

Совершенствование законодательства

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации

п. 19.1. Актуализация сведений
п. 19.2. Мониторинг представления актуальности и достоверности сведений
п. 19.3. Привлечение к мониторингу подведомственных организаций

п. 10. Исходными данными для категорирования являются:
ж) перечни типовых отраслевых объектов КИИ *(с 21 марта 2023 г.)*

Уточнены показатели критериев значимости объектов КИИ РФ и их значения

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации *(приказ ФСТЭК России от 25.12.2017 № 239)*

29.2. СЗИ (не встроенные) должны соответствовать *6* или более высокому уровню доверия.

29.3. Прикладное ПО, планируемое к внедрению в рамках создания, модернизации, реконструкции, ремонта ЗО и обеспечивающее выполнение его функций, должно соответствовать следующим требованиям по безопасности:

- 29.3.1. Требования по безопасной разработке ПО
- 29.3.2. Требования к испытаниям по выявлению уязвимостей в ПО
- 29.3.3. Требования к поддержке безопасности ПО

29.4. Выполнение требований, оценивается на этапе проектирования ЗО на основе анализа материалов и документов, представляемых разработчиком

Типовые нарушения

- использование ПО с большим количеством известных уязвимостей критического и высокого уровня опасностей
- субъектами не проводится анализ защищенности
- на технических средствах, ПО и ПАК, стоят пароли по умолчанию
- меры, которые реализует субъект, в ряде случаев являются формальными. При этом, в случае невозможности реализации тех или иных средств защиты, организации не применяют компенсирующие меры
- отсутствует контроль за действиями внешних организаций в системах
- используются неучтенные носители информации
- не отключаются неиспользуемые порты и интерфейсы

! Зачастую критические объекты подключаются к корпоративным системам. Формально вы считаете, что выхода в интернет у них нет, однако корпоративная система, зачастую без применения средств защиты информации, взаимодействует с интернетом.

! Еще одна ситуация – когда зависимые друг от друга объекты имеют разные категории. Все подсистемы, которые работают с критическими объектами, должны соответствовать их категории и иметь соответствующие меры безопасности

ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР исследования безопасности ядра LINUX

В 2022 году

Создан технологический центр исследования безопасности операционных систем, созданных на базе ядра Linux

Проведена опытная эксплуатация технологического центра исследования безопасности операционных систем, созданных на базе ядра Linux

Подготовлены сведения об уязвимостях, а также исправления, устраняющие уязвимости в операционных системах, созданных на базе ядра Linux

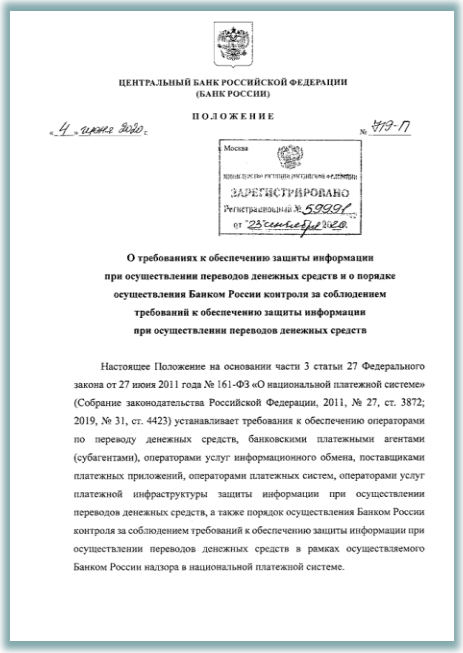
Активности Технологического центра включают:

- Разработку методик применения лучших практик разработки безопасного ПО
- Доработку ядра Linux с целью повышения его безопасности
- Разработку патчей по устранению уязвимостей в ядре Linux
- Наполнение БДУ ФСТЭК России сведениями об уязвимостях ядра Linux
- Подготовку рекомендаций по безопасному использованию ядра
- Подготовку отечественных специалистов, участвующих в разработке ядра Linux

Защита информации в платежной системе

Указание Банка России от 18 февраля 2022 г. №6071-У фактический **запрет на широкое использование ПЭП** для подтверждения транзакций в финансовых операциях с переходом на УНЭП, или УКЭП, или СКЗИ с функцией имитозащиты

В связи с принятием Указа Президента РФ №250 сроки **полного перехода на российские СКЗИ при осуществлении защиты в платежах** (Положение ЦБ №719-П) сокращаются **с 1 января 2031 г. до 1 января 2025 г.**



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«4» июня 2020 г. № 719-П

г. Москва

ЗАРЕГИСТРИРОВАНО
Регистрационный № 59991
от "25" сентября 2020 г.

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

ИБ как отдельная отрасль

Приказ Росстандарта от 3 апреля 2023 года № 178-ст «Об утверждении Изменения к Общероссийскому классификатору видов экономической деятельности…

Выделено 10 НОВЫХ КОДОВ ОКВЭД2 для ИБ в частности:

- производство средств защиты конфиденциальной информации
- деятельность по аттестационным испытаниям и аттестации на соответствие требованиям по ЗИ
- деятельность по контролю защищенности конфиденциальной информации от утечки по техническим каналам, от НСД и ее модификации
- деятельность по мониторингу ИБ средств и систем информатизации
- деятельность по обеспечению ЗИ

ВОЗМОЖНЫЕ ПРЕИМУЩЕСТВА

- ✓ оформление налоговых льгот конкретно для организаций, занимающихся ИБ.
- ✓ отнесение к отрасли ИБ организаций, занимающихся проведением аттестационных испытаний, контролем защищенности, мониторингом, тематическими исследованиями и т.д.

Налоговые льготы. Изменения в Налоговый Кодекс

В 2022-2024 годах устанавливается НАЛОГОВАЯ СТАВКА по налогу в размере 0% для организаций, осуществляющих деятельность в ИТ-области

Минцифры России планирует продлить льготы после 2024 года

ВАЖНО для производителей ПАК. Ставка действует, если доходы организации:

1. **от оказания услуг** (выполнения работ) по разработке (включая тестирование и сопровождение) ПАКов …, а также по адаптации, модификации, тестированию и сопровождению ПАКов, включенных в единый реестр российских программ для ЭВМ и БД
2. **от реализации** разработанных данной организацией ПАКов, включенных в единый реестр российских программ для ЭВМ и БД

составляют не менее 70% всех доходов организации

Изменения в области ПДн

Роскомнадзором утверждены Требования к оценке вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных» (приказ РКН №178, 2022г.)

Определены:

- ответственный за оценку вреда
- степень вреда (высокая, средняя, низкая)
- критерии отнесения вреда к одной из степеней
- правила оформления результатов оценки

Федеральный закон №625-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

ПРИНЯТО

КоАП

Разрешается составлять протоколы об административных правонарушениях за нарушения в области персональных данных без проведения контрольных (надзорных) мероприятий во взаимодействии с контролируемым лицом

Штраф за утечку ПДн
от 5 млн.руб.
до 500 млн.руб.

НА РАССМОТРЕНИЕ

Апрельские тезисы

Биометрические персональные данные

Положение о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации
(ПП от 11.04.2023 № 585)
Госконтроль осуществляет Минцифры.
Положением установлены:
- ✓ плановые контрольные мероприятия и периодичность их проведения
- ✓ виды профилактических мероприятий, которые могут проводиться при осуществлении государственного контроля

Порядок обращения с документами ДСП

Минцифры подготовлен проект ПП «Об утверждении Положения о порядке обращения с документами ДСП в ФОИВ, госкорпорациях, а также подведомственных им организациях»
Устанавливаются:
- ✓ требования к порядку создания документов ДСП
- ✓ требования к внутреннему порядку обращения с документами ДСП
- ✓ требования к обеспечению защиты информации при работе с документами ДСП и ответственность за нарушение положения

Лицензионный контроль

Проекты приказов ФСТЭК России
Об утверждении сроков и последовательности административных процедур при осуществлении ФСТЭК России лицензионного контроля за деятельностью по:
- ✓ технической защите конфиденциальной информации
- ✓ разработке и производству средств защиты КИ

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

Ответы на вопросы

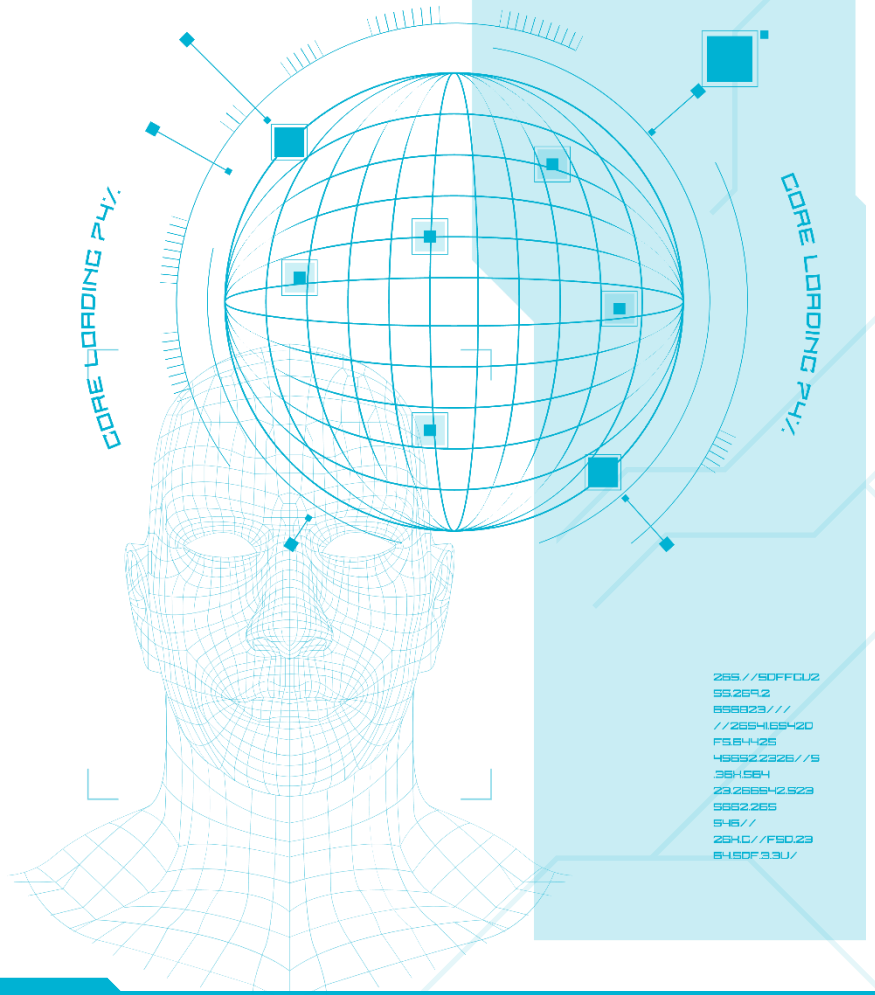
Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363

ССЫЛКИ


CORE LOADING 24%
CORE LOADING 24%
255.//9DFFGU2
55.2652
555823.///
//2654165420
F5.64425
45652.2326.//5
35H.554
23.2665425.23
5852.265
546//
25HC//F50.23
6H50F3.3U/

1. Указ Президента от 30.03.2022 №166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» - http://publication.pravo.gov.ru/Document/View/0001202203300001
2. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» - http://publication.pravo.gov.ru/Document/View/0001202205010023?index=0&rangeSize=1
3. Проект Указа Президента Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» - https://regulation.gov.ru/projects#npa=135259
4. Проект приказа ФСБ России «Об утверждении Порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, … либо используемых ими» - https://regulation.gov.ru/projects#search=Порядка%20осуществления%20мониторинга%20защищенности%20информационных%20ресурсов&npa=133499
5. Распоряжение Правительства РФ от 29 марта 2023 г. N 757-р - http://publication.pravo.gov.ru/Document/View/0001202303300060
6. Постановление Правительства Российской Федерации от 15.07.2022 № 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» - http://publication.pravo.gov.ru/Document/View/0001202207190035
7. Приказ ФСБ России от 01.11.2022 г. № 543 «Об определении переходного периода, предусмотренного подпунктом "б" п. 5 Указа Президента Российской Федерации № 250» - http://publication.pravo.gov.ru/Document/View/0001202212020034
8. Приказ ФСБ России от 24 октября 2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» - http://publication.pravo.gov.ru/Document/View/0001202211230034
9. Приказ ФСБ России от 04.11.2022 г. № 547 «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации» - http://publication.pravo.gov.ru/Document/View/0001202211170017
10. Постановление Правительства Российской Федерации от 20.12.2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» - http://publication.pravo.gov.ru/Document/View/0001202212210032
11. Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» - http://publication.pravo.gov.ru/Document/View/0001202211290008

12. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателе критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» - http://publication.pravo.gov.ru/Document/View/0001201802130006
13. Постановление Правительства Российской Федерации от 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц» … » - http://publication.pravo.gov.ru/Document/View/0001202208260051
14. Приказ ФСБ России от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» - http://publication.pravo.gov.ru/Document/View/0001202211230034
15. Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных» - http://publication.pravo.gov.ru/Document/View/0001202211290004
16. Постановление Правительства Российской Федерации от 20.12.2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» - http://publication.pravo.gov.ru/Document/View/0001202211290008
17. Постановление Правительства Российской Федерации от 08.12.2022 № 2250 "О внесении изменения в Положение о защите информации в платежной системе" - http://publication.pravo.gov.ru/Document/View/0001202212090032
18. Приказ ФСБ России от 04.11.2022 № 547 "Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации" - http://publication.pravo.gov.ru/Document/View/0001202211170017
19. Проект приказа ФСТЭК России «Об утверждении Порядка осуществления Федеральной службой по техническому и экспортному контролю лицензирования деятельности по технической защите конфиденциальной информации» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134091
20. Приказ ФСТЭК России от 12.01.2023 № 4 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 133 и внесенных в него изменений» - http://publication.pravo.gov.ru/Document/View/0001202302030009

21. Проект приказа ФСТЭК России «Об утверждении Порядка осуществления Федеральной службой по техническому и экспортному контролю лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134170
22. Приказ ФСТЭК России от 12.01.2023 № 3 "Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений"- http://publication.pravo.gov.ru/Document/View/0001202302030006
23. Проект приказа ФСТЭК России «Об утверждении Регламента осуществления Федеральной службой по техническому и экспортному контролю функции по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации» – https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134355
24. Проект приказа ФСТЭК России «Об утверждении Регламента осуществления Федеральной службой по техническому и экспортному контролю функции по лицензированию деятельности по технической защите конфиденциальной информации» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134356
25. Проект приказа ФСТЭК России «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134466
26. Проект приказа ФСТЭК России «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=134468
27. Приказ ФСТЭК России от 27.11.2022 г. N 187 «Об утверждении требований по безопасности информации к средствам виртуализации» - https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-27-oktyabrya-2022-g-n-187
28. Приказ ФСТЭК России от 04.07.2022 г. N 118 «Об утверждении требований по безопасности информации к средствам контейнеризации» - https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-4-iyulya-2022-g-n-118
29. Приказ ФСТЭК России от 19.09.2022 № 172 «О внесении изменений в Положение о системе сертификации средств защиты информации, утвержденное приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. № 55» - http://publication.pravo.gov.ru/Document/View/0001202210190024

30. Проект постановления Правительства Российской Федерации «О внесении изменений в Положение о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации, утвержденное постановлением Правительства Российской Федерации от 11 октября 2021 г. № 1729» - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=135061
31. Приказ Минцифры России от 12.09.2022 № 659 «Об утверждении требований к линиям связи, пересекающим Государственную границу Российской Федерации, и к средствам связи, к которым подключаются указанные линии связи» - http://publication.pravo.gov.ru/Document/View/0001202211290036
32. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» - http://publication.pravo.gov.ru/Document/View/0001202212290024
33. Проект приказа ФСБ России «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по лицензированию деятельности по разработке, производству, распространению шифровальных (криптографических) средств, … » - https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=132843
34. Распоряжение Правительства РФ от 15.11.2022 № 3461-р «Об утверждении Перечня сведений, включенных в реестр линий связи, пересекающих государственную границу РФ, и средств связи, с которым подключаются указанные линии связи, содержащий информацию, которая является общедоступной»- http://publication.pravo.gov.ru/Document/View/0001202211150029
35. Законопроект №244043-8 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» - https://sozd.duma.gov.ru/bill/244043-8
36. Требования по безопасности информации к средствам контейнеризации утверждены Приказом ФСТЭК России от 04.07.2022 г. № 118 - https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-4-iyulya-2022-g-n-118
37. Требования по безопасности информации к средствам виртуализации утверждены Приказом ФСТЭК России от 02.10.2022 г. № 187 – https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-27-oktyabrya-2022-g-n-187
38. Указание Банка России от 18.02.2022 №6071-У «О внесении изменений в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» - https://cbr.ru/Queries/UniDbQuery/File/90134/2591
39. Информационное письмо Банка России №ИН-017-56/22 от 16.03.2023 «Информационное письмо о применении требований нормативных актов Банка России об обеспечении целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом Банк России» - http://www.cbr.ru/crosscut/lawacts/file/6158

2023 infotecs
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

При поддержке