



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ

08 ДЕКАБРЯ 2022

АНАЛИЗ РЕГУЛЯТОРИКИ В 2022

НИКОЛАЙ КАЗАНЦЕВ, SECURITM.RU



МОСКВА



- 
- ПДн
 - 250
 - КИИ
 - ГИС
 - ФСТЭК
 - Финансы
 - СУИБ
 - ГОСТЫ



- ЕБС
- УЦ/ЭП
- Аккредитация
- Сертификация
- Аттестация

#ПДН



Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" ...

Уведомления РКН в
большом количестве
случаев

Детализация **перечня**
ПДн при передаче

Построение
документов вокруг
цели обработки

Порядок **оценки**
негативных
последствий

Взаимодействие с
ГосСОПКА

Уведомление РКН об
утечках ПДн

Ограничения на
трансграничную
передачу

Запрет на
обязательность
биометрии

#ПДН

Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" ...

Приказ РКН от 27.10.2022 № 178
«Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ

Приказ РКН от 28.10.2022 № 179
«Об утверждении Требований к подтверждению уничтожения ПДн»

Приказ РКН от 05.08.2022 № 128
«Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн»..

#ПРОЕКТ Приказ РКН
Об утверждении форм уведомлений о намерении осуществлять обработку ПДн, о внесении изменений в ранее представленные сведения, о прекращении обработки персональных данных

#ПРОЕКТ Приказ РКН
Об утверждении Порядка и условий взаимодействия РКН с операторами в рамках ведения реестра учета инцидентов в области ПДн

#ПРОЕКТ Приказ РКН + ФСБ
Об утверждении Порядка передачи информации о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) ПДн

#ПРОЕКТ ПП РФ
Об утверждении Порядка принятия решений о запрещении или об ограничении трансграничной передачи ПДн в целях защиты нравственности, здоровья, прав и законных интересов граждан

#ПРОЕКТ ПП РФ
Порядок принятия решений о запрещении или об ограничении трансграничной передачи ПДн по представлению уполномоченного органа



#ПДН

РОСКОМНАДЗОР

ПОРТАЛ ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

[Главная](#)

[Об уполномоченном органе](#)

[Реестр нарушителей](#)

[Кодекс добросовестных практик](#)

[Реестр операторов](#)

[Инциденты \(утечки ПД\)](#)

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

[Проверка состояния уведомления](#)

[Трансграничная передача](#)

[Молодежная палата Консультативного совета](#)

[Электронная библиотека по защите прав субъектов персональных данных](#)

[Согласие на обработку ПД, разрешенных для распространения](#)

[Главная страница](#) > [Инциденты \(утечки ПД\)](#)

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Подать уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Пройти аутентификацию на портале Госуслуг, заполнить форму и направить ее в электронном виде. У Вас должна быть подтвержденная учетная запись. Отправка копии в бумажном виде в данном случае не потребуется. В случае если Вы подаете уведомление за организацию, ваша учетная запись должна быть привязана к данной организации на портале Госуслуг.

[перейти к сервису ЕСИА](#)

Подать уведомление о результатах внутреннего расследования

Ранее при подаче уведомления о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Вам направлено информационное письмо, содержащее номер и ключ уведомления.

Для предоставления дополнительной информации о результатах внутреннего расследования инцидента Вам необходимо заполнить поля, указав номер и ключ уведомления.

Заполняя указанную форму, Вы подтверждаете, что являетесь лицом, уполномоченным на предоставление информации о результатах внутреннего расследования инцидента.

[перейти к сервису ЕСИА](#)

#250

УП РФ от 01.05.2022 № 250
"О дополнительных мерах по обеспечению информационной безопасности
Российской Федерации"

Возложение
ответственности за ИБ
на **зам. руководителя**

Привлечение
аккредитованных
центров ГосСОПКА

Проведение **оценки**
защищенности
ключевыми органами

Запрет СЗИ из
недружественных стран
с 01.01.25

ПП РФ от 15.07.2022 №1272

Об утверждении типового
положения о заместителе
руководителя ...

Приказ ФСБ от 07.07.2022
N 348

О внесении изменений в
Порядок информирования
ФСБ России о компьютерных
инцидентах

Минцифры

Типовое техническое задание
на выполнение работ по
оценке уровня
защищенности
информационной
инфраструктуры

Распоряжение Правительства
РФ от 22.06.2022 № 1661-р

Об утверждении перечня
ключевых органов
(организаций), которым
необходимо осуществить
мероприятия по оценке
уровня защищенности ...

#КИИ

УП РФ от 30.03.2022 № 166

О мерах по обеспечению технологической независимости и безопасности КИИ РФ

ПП РФ от 22.08.2022 № 1478

Об утверждении требований к ПО, в том числе в составе ПАК, используемому органами государственной власти, заказчиками, осуществляющими закупки ...

Приказ ФСБ от 07.07.2022 № 348

О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах ...

ПП РФ от 19.08.2022 № 1463

О внесении изменения в Правила категорирования объектов КИИ РФ

ФЗ от 14.07.2022 № 255-ФЗ

О контроле за деятельностью лиц, находящихся под иностранным влиянием

Приказ ФСТЭК от 10.02.2022 № 26

О внесении изменений в Порядок ведения реестра значимых объектов КИИ РФ

#ГИС

Приказ ФСБ от 24.10.2022 № 524

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



ПП РФ от 13.05.2022 г. № 860

О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений



Минздрав России

Концепция информационной безопасности в сфере здравоохранения



#ФСТЭК

Новая БДУ ФСТЭК

Методика оценки
угроз безопасности
информации

Методический документ ФСТЭК от 28.10.2022
Методика оценки уровня **критичности уязвимостей**
программных, программно-аппаратных средств

Методический документ ФСТЭК от 28.10.2022 года
Методика **тестирования обновлений** безопасности
программных, программно-аппаратных средств

#ФСТЭК



пример



УБИ.2.1.1 Угроза несанкционированного доступа к автоматизированному рабочему месту за счет эксплуатации уязвимостей

#Финансы

802-П от 25.07.2022

О требованиях к защите информации в платежной системе Банка России

719-П от 04.06.2020 (вступил с 01.01.2022)

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств ...

716-П (УБР от 25.03.2022 №6103-У)

О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

683-П (УБР от 18.02.2022 №6071-У)

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

747-П

О требованиях к защите информации в платежной системе Банка России

382-П

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств ...



#Финансы



Операционная надежность

ПБР № 787-П от 12.01.2022

Обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг

ПБР № 779-П от 15.11.2021

Обязательные для некредитных финансовых организаций требования к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке"

#Финансы



SWIFT Customer Security
Controls Framework v2022

27 требований



Payment Card Industry
Data Security Standard 4.0
от 01.03.2022

250 требований

#СМИБ/СУИБ/ISMS

ISO/IEC 27001:2013
"Information technology -
Security techniques -
Information security
management systems -
Requirements"



ГОСТ Р ИСО/МЭК 27001-2021 01.01.2022
Информационная технология. Методы и средства
обеспечения безопасности. Системы менеджмента
информационной безопасности. Требования.



ISO/IEC 27001:2022(E) 25.10.2022
Information security, cybersecurity and privacy protection
— Information security management systems —
Requirements



#ГОСТы



Защита информации. Управление компьютерными инцидентами.

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

- ГОСТ Р 59548-2022 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации
- ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации
- ПНСТ 799-2022 Информационные технологии. Криптографическая защита информации. Термины и определения



НКЦКИ

ФИНЦЕРТ

ФСТЭК

ЦБР

НСПК



Анализ требований



Garza

BRUNNEN

BRUNNEN
MUSIK

1 2 3 4 5 6 7 8 9 10 11 12
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z

NERA

HA VEI DREI AM
ENGO UN SUEÑO

RENAN
España en China

ALBERTO CAMPO BAEZA

ky

THE GREAT

RENAN

Документ	gost-57580-1-2017-part9	gost-57580-1-2017-part8	sto-br-ibbs-10-2014	cis-csc-8	polozhenie-banka-rossii-787-p	gost-57580-1-2017-part7	fstec-21	iso-27001	guideline-for-a-healthy-information-system	iso27001-annex-a	cis-csc-7	pci-dss-v4-0-ru	fstec-17	strategies-to-mitigate-cyber-security-incidents	cscf-v2022	fstec-31	polozhenie-br-757p	polozhenie-br-779p	polozhenie-br-683p	nist-csf-en	rs-dr-ibbs-25-2014	fstec-239
gost-57580-1-2017-part9		0	0	0	8	0	3	0	6	25	0	30	2	3	5	3	6	7	1	0	0	4
gost-57580-1-2017-part8	0		0	0	0	0	5	0	9	10	0	35	5	1	5	20	20	0	3	0	0	19
sto-br-ibbs-10-2014	0	0		0	25	1	0	0	59	114	0	140	0	9	29	2	19	23	11	0	0	3
cis-csc-8	0	0	0		8	1	1	0	60	122	106	114	1	44	15	4	1	8	1	76	0	2
polozhenie-banka-rossii-787-p	8	0	25	8		6	10	0	1	15	8	15	6	2	5	12	1	1	2	18	2	14
gost-57580-1-2017-part7	0	0	1	1	6		206	0	106	147	0	241	202	50	38	214	7	6	5	0	0	224
fstec-21	3	5	0	1	10	206		0	31	62	1	97	94	32	45	39	7	10	4	1	0	41
iso-27001	0	0	0	0	0	0	0		3	1	0	4	0	0	1	0	0	0	0	35	0	0
guideline-for-a-healthy-information-system	6	9	59	60	1	106	31	3		40	53	23	20	22	18	37	3	1	0	35	0	37
iso27001-annex-a	25	10	114	122	15	147	62	1	40		204	158	64	11	36	75	7	13	4	285	40	71
cis-csc-7	0	0	0	106	8	0	1	0	53	204		79	1	47	19	4	0	7	0	125	0	2
pci-dss-v4-0-ru	30	35	140	114	15	241	97	4	23	158	79		91	12	67	111	5	10	11	140	21	115
fstec-17	2	5	0	1	6	202	94	0	20	64	1	91		27	37	87	4	6	2	0	0	78
strategies-to-mitigate-cyber-security-incidents	3	1	9	44	2	50	32	0	22	11	47	12	27		11	32	0	2	0	29	0	32
cscf-v2022	5	5	29	15	5	38	45	1	18	36	19	67	37	11		39	0	5	1	51	4	39
fstec-31	3	20	2	4	12	214	39	0	37	75	4	111	87	32	39		9	14	6	0	0	100
polozhenie-br-757p	6	20	19	1	1	7	7	0	3	7	0	5	4	0	0	9		1	9	1	5	7
polozhenie-br-779p	7	0	23	8	1	6	10	0	1	13	7	10	6	2	5	14	1		2	23	2	16
polozhenie-br-683p	1	3	11	1	2	5	4	0	0	4	0	11	2	0	1	6	9	2		1	0	7
nist-csf-en	0	0	0	76	18	0	1	35	35	285	125	140	0	29	51	0	1	23	1		0	0
rs-dr-ibbs-25-2014	0	0	0	0	2	0	0	0	0	40	0	21	0	0	4	0	5	2	0	0		0
fstec-239	4	19	3	2	14	224	41	0	37	71	2	115	78	32	39	100	7	16	7	0	0	

ТОП 10 требований/процессов ИБ

01 Защита сети

02 Логирование

03 Антивирусная защита

04 Управление инцидентами

05 Инвентаризация

06 Управление уязвимостями

07 Обучение персонала

08 Защита учетных записей

09 Аутентификация

10 Физическая безопасность



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ

08 ДЕКАБРЯ 2022

АНАЛИЗ РЕГУЛЯТОРИКИ В 2022

НИКОЛАЙ КАЗАНЦЕВ, SECURITM.RU



МОСКВА

