АКТУАЛЬНЫЕ ЗАДАЧИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В 2023 ГОДУ

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности

ЧТО ПРОИСХОДИТ?

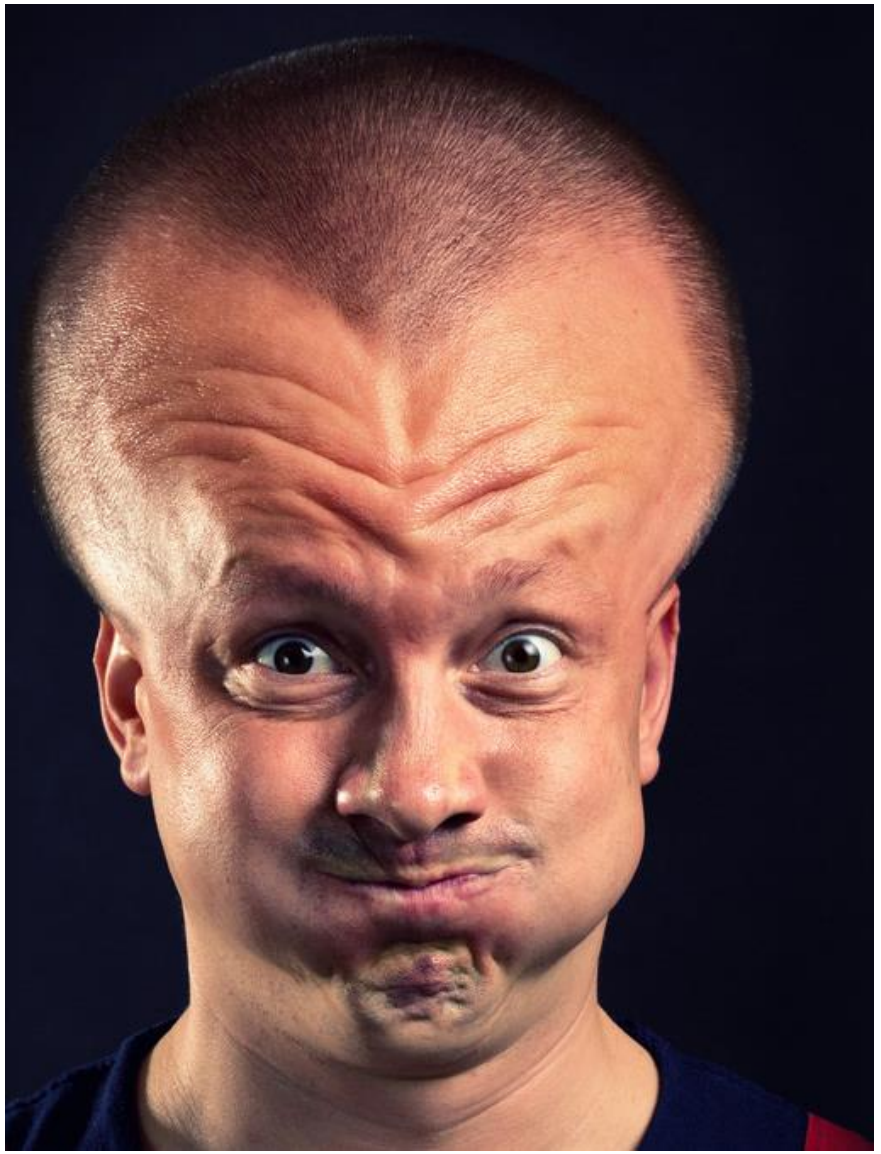
Массированные компьютерные атаки на информационную инфраструктуру:

- Отказ в обслуживание сервисов и каналов связи
- Дискредитация репутации
- Фишинг, атаки на сотрудников
- Атаки через подрядчиков

Реализация мер по обеспечению технологической независимости: Указ Президента от 30 марта 2022 г. № 166, постановление Правительства от 22 августа 2022 г. № 1478

Усиление требований к безопасности ПДн и КИИ:

- Изменения в 152-ФЗ «О персональных данных»
- Оборотные штрафы (по принципу GDPR)
- Уголовная ответственность за передачу/разглашение ПДн
- Оценка соответствия СрЗИ в части ЗОКИИ
- Безопасная разработка
- Пересмотр категории ОКИИ



КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Массированные компьютерные атаки на информационную инфраструктуру

Что происходит?	Что делать?
Отказ в обслуживании сервисов и каналов связи	АнтиDDOS (от провайдера)
Дискредитация репутации	Заведение внешних ресурсов за WAF, OSINT
Фишинг, атаки на сотрудников	Повышение осведомленности, антифишинговые тренировки, киберучения
Атаки через подрядчиков	• ответственность на уровне договоров; • мониторинг и подключение через СКДП • Проведение работ только после согласования (по возможности)

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Технологическая независимость

Что делать?
Разработка плана перехода на использование Российского ПО под соответствующую категорию субъекта. Для всех - ЗОКИИ.
Разработать и отправить в Минцифры РФ – до 18 марта
При подготовке раздела 2 плана – показатели эффективности – использовать отраслевой план
То же самое при переходе на ДПАК

УТВЕРЖДЕНЫ
приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации
от 18 января 2023 г. № 21

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Изменения в 152-ФЗ «О персональных данных»

Изменение	Чего касается?	Что делать?
Изменения с 01.03.2023		
Оператор обязан провести оценку вреда в соответствии с требованиями, установленными Роскомнадзором, который может быть причинен субъектам ПДн в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ	Оценка вреда, который может быть причинен субъектам ПДн	Готовить акты оценки вреда в соответствии с приказом Роскомнадзора от 27.10.2022 N 178 (01.03.23-01.03.29)
Подтверждение уничтожения ПДн в случаях, предусмотренных ст. 21 152-ФЗ, осуществляется в соответствии с требованиями, установленными Роскомнадзором	Уничтожение ПДн	Скорректировать требования к акту уничтожения в соответствии с приказом Роскомнадзора от 28.10.2022 N 179 (01.03.23-01.03.29)
Уведомлять Роскомнадзор об изменениях оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения. В случае прекращения обработки ПДн оператор обязан уведомить в течение 10 рабочих дней с даты прекращения обработки ПДн	Изменения в уведомлении Роскомнадзор	Скорректировать сроки процедуры актуализации уведомления
– **РКН утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн. В перечень включаются государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц, а также иностранные государства, не являющиеся сторонами Конвенции Совета Европы** – **Оператор до начала осуществления трансграничной передачи обязан уведомить РКН о своем намерении. Уведомление направляется отдельно от уведомления о намерении осуществлять обработку ПДн.** – **Оператор до подачи уведомления обязан получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача персональных данных, ряд сведений.** – **РКН может запретить или ограничить трансграничную передачу.**	Трансграничная передача ПДн	Перечень утвержден Приказом Роскомнадзора от 05.08.2022 N 128 (вступает в силу 01.03.23) Уведомить о том, что осуществляете/планируете осуществлять трансграничную передачу Распространяется не на все организации
ПРИКАЗ РКН от 14 ноября 2022 г. № 187 • **Что должное содержаться в уведомлении об инциденты** • **Подается или в форме бумажного документа, или через портал РКН** • **Инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшие нарушение прав субъектов персональных данных**	Взаимодействие РКН с операторами ПДн в рамках **инцидентов**	Корректировка положения об управлении инцидентами, положения о взаимодействии с государственными/надзорными органами.
Приказ ФСБ России от 13 февраля 2023 года № 77: • **СуКИИ и иные органы и организации взаимодействующие с НКЦКИ – по уже имеющимся каналом с применением форматов НКЦКИ, в течение 24 часов с момента обнаружения** • **Иные операторы – путем заполнения формы на портале РКН, не позднее 24 часов с момента обнаружения, не позднее 72 часов с момента обнаружения о результатах внутреннего расследования** • **Оператор вправе обратиться за помощью в расследовании в НКЦКИ** • **НКЦКИ может отправлять запросу с уточнениями по инциденту на которые оператор обязан отвечать в течении 24 часов.**	Взаимодействие с ГосСОПКА операторами ПДн в рамках **компьютерных инцидентов**	Корректировка положения об управлении инцидентами, положения о взаимодействии с государственными/надзорными органами. Корректировка документации по КЦ ГосСОПКА

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Усиление требований к безопасности КИИ

с 1 января 2023 года вступили в силу требования Приказа ФСТЭК России от 20.02.2020 №35, вносящего изменения и дополнительные меры в Требования по обеспечению безопасности значимых объектов КИИ, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239:

Необходимость соответствия **наложенных** СрЗИ по 6 или более высокому УД

Сертификация/применение сертифицированных СрЗИ →

- Создание нового ЗОКИИ
- Модернизация (в рамках отдельного ЧТЗ) ЗОКИИ
- Замена текущих (внедренных до 01.01.2023) средств защиты информации: замена на аналог, смена версии, покупка новых лицензий

Общесистемное ПО – соответствие СрЗИ требованиям установленным в ТЗ на создание ЗОКИИ или его подсистемы безопасности

Прикладное ПО (создание, модернизация, реконструкция/ремонт):

- требованиям по безопасной разработке (DevSecOps)
- требованиям к испытаниям по выявлению уязвимостей в программном обеспечении: SAST, DAST, Fuzzing
- требованиям к поддержке безопасности программного обеспечения

→ Выполнение требований оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции, ремонту) или обеспечению безопасности ЗОКИИ, на этапе проектирования на основе документации разработчика ПО.

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

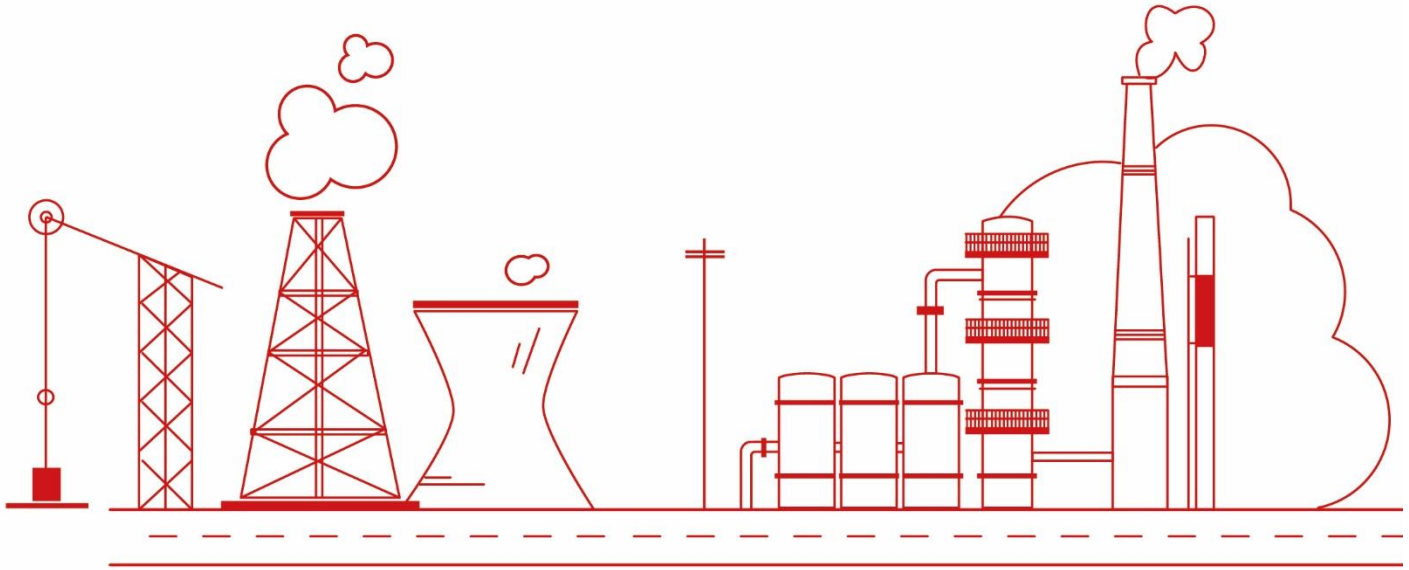
Усиление требований к безопасности КИИ

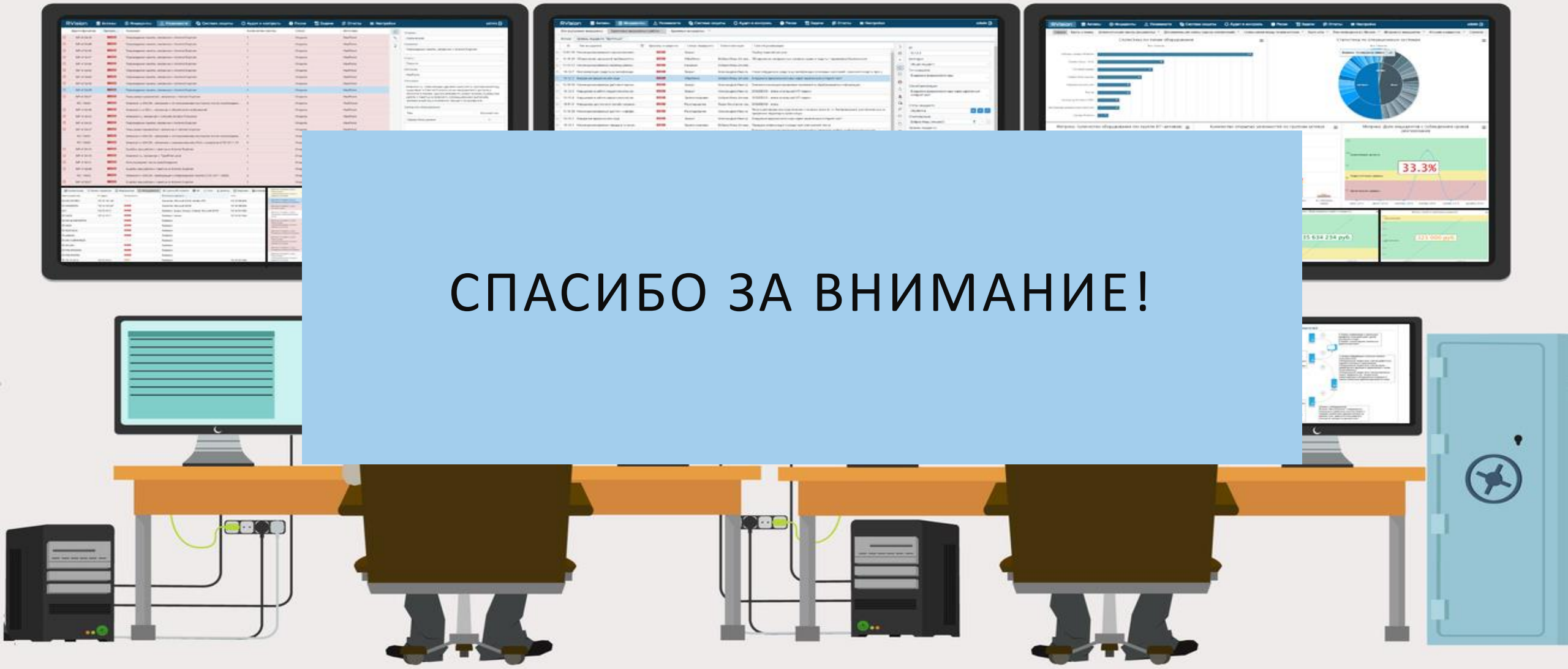
Постановление Правительства РФ от 20.12.2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127». В соответствии с п. 21 Правил категорирования – **пересмотр** категорий значимости.

Для ЗОКИИ 1 КЗ ничего не меняется

Для ОКИИ других категорий/без категории:

- оценка применимых к объектам КИИ показателей критериев значимости;
- сравнение ранее полученных значений по каждому из рассчитываемых показателей критериев значимости с изменениями в перечне показателей критериев значимости;
- фиксация принятых решений актами;
- после утверждения актов, в случае если у объекта (объектов) КИИ произошло изменение категории значимости, во ФСТЭК России направляются сведения о категорировании по установленной форме.





СПАСИБО ЗА ВНИМАНИЕ!

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности