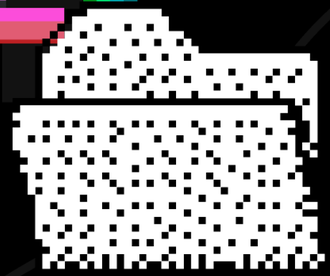
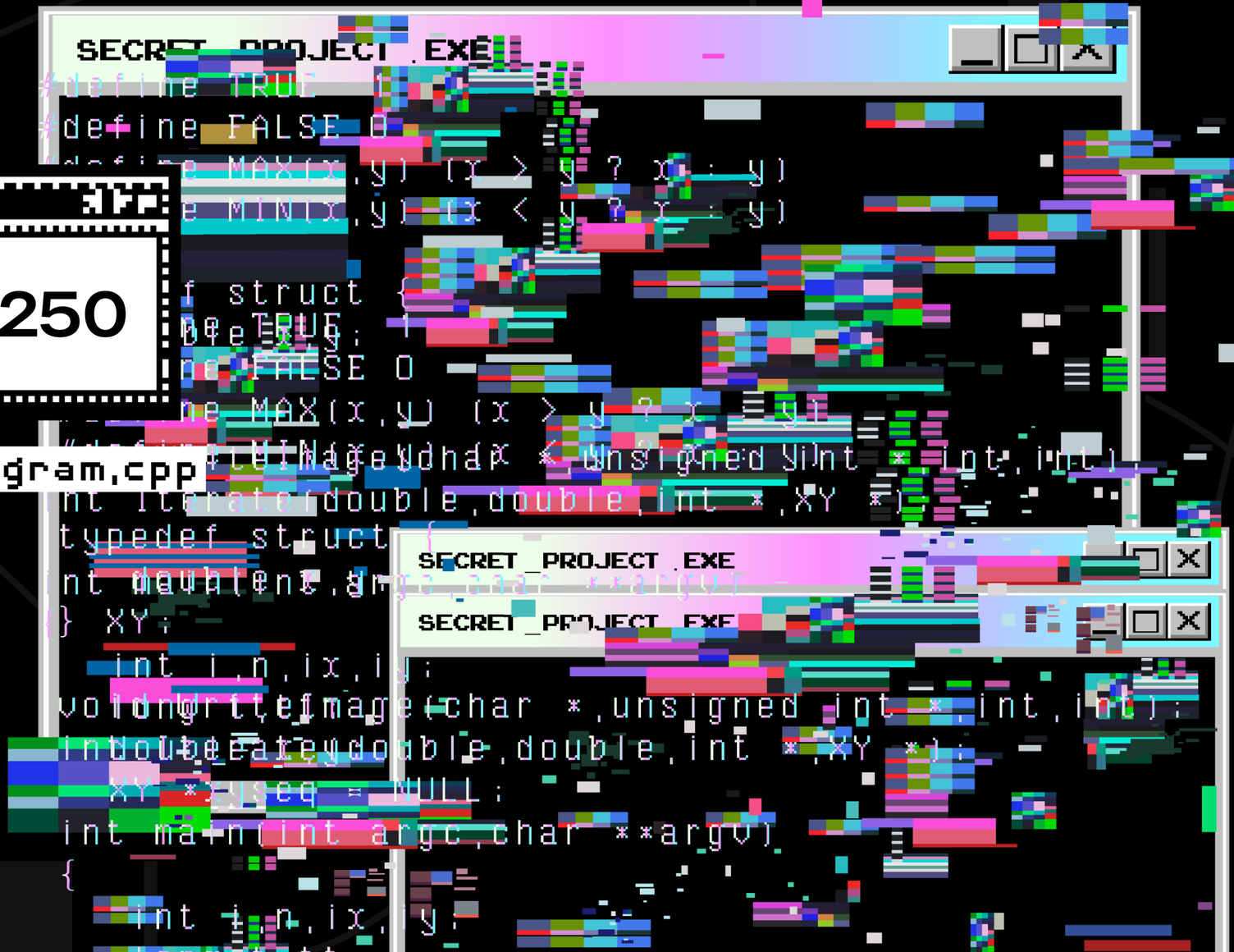
Указ Президента РФ №250 — от А до Я



local_files

#250

myprogram.cpp



Алексей Лукацкий

Ключевые идеи Указа № 250

1. **Руководитель организации** должен ответить/отвечать за ИБ и у него должны быть «руки» для этого!

2. Средств защиты **из недружественных стран** (а в перспективе и из иных иностранных) быть не должно!

3. ИБ должна быть **практической и результативной,** а не «для галочки», учитывающей потребности и задачи бизнеса/госуправления

На кого распространяется

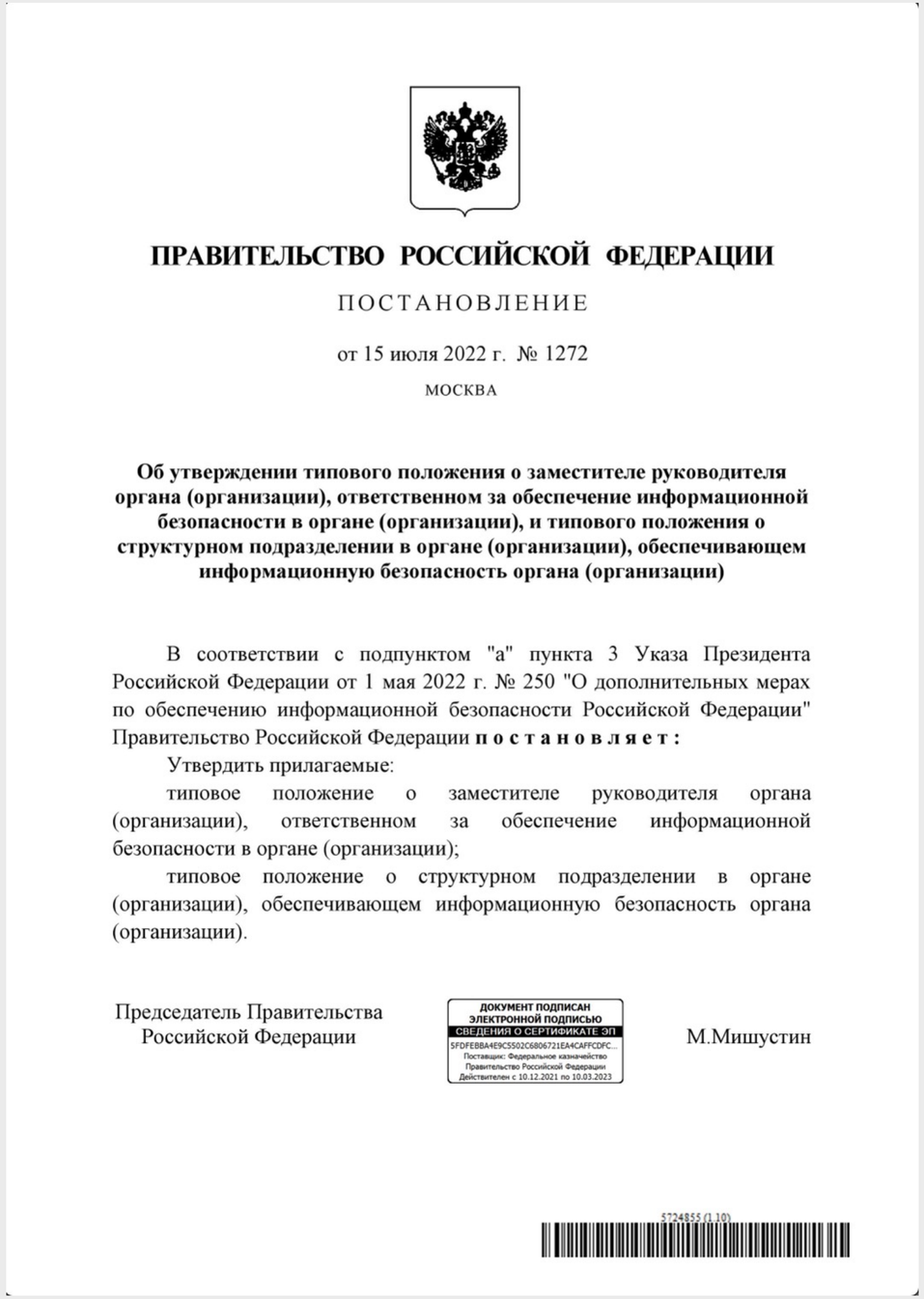
- Органы госвласти
- Высшие исполнительные органы госвласти
- Госфонды
- Госкорпорации
- Иные предприятия, созданные на основании ФЗ
- Стратегические предприятия и стратегические акционерные общества
- Системообразующие организации экономики
- Субъекты КИИ

В первоначальной версии субъекты КИИ не упоминались вообще

Всего организаций, попавших под действие Указа, более 500 тысяч

Постановление Правительства РФ №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)»



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

МОСКВА

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)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

Председатель Правительства Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
5FDFEBBA4E9C5502C6806721EA4CAFFCDFC...
Поставщик: Федеральное казначейство
Правительство Российской Федерации
Действителен с 10.12.2021 по 10.03.2023

М.Мишустин

5724855 (1.10)

Образование ответственного лица

Высшее профильное или **Профпереподготовка**

- 10.03.01 «Информационная безопасность»
- 10.05.01 «Компьютерная безопасность»
- 10.05.02 «ИБ телекоммуникационных систем»
- 10.05.03 «ИБ автоматизированных систем»
- 10.05.04 «Информационно-аналитические системы безопасности»
- 10.05.05 «Безопасность ИТ в правоохранительных органах»

- Минимальный срок профессиональной переподготовки – 250 академических часов

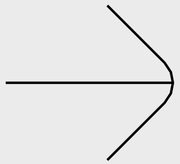
  п. 12 Приказа Министерства образования и науки РФ № 499 от 01.07.2013 г.

- Минимальный срок освоения программ профессиональной переподготовки в области информационной безопасности – не менее 360 часов

  п. 17 Приказа Министерства образования и науки РФ № 1316 от 19.10.2020 г.

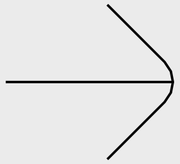
Два вопроса по ответственному

Нужно ли согласование программ проф-переподготовки?



По приказу Минобразования №1316 да, по Указу Президента РФ - нет

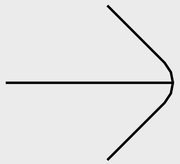
А можно топ-менеджеру не учиться 360 часов?



Сейчас рассматривается вопрос разделения требований по уровню компетенций и образования для заместителя руководителя организации и руководителя подразделения ИБ, а пока да ☹

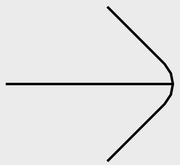
Два вопроса по подразделению ИБ

А можно возложить на ИТ-подразделение?



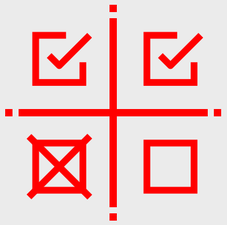
Да, можно (исключая финансовые организации, которым это запрещает новая редакция 716-П)

А можно не создавать и все аутсорсить?

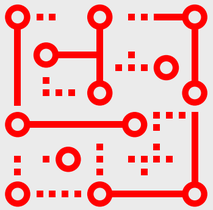


В случае нехватки специалистов возможно поручение данной задачи внешней организации – лицензиату ФСТЭК, но контроль за соблюдением Указа и аутсорсера должен быть реализован все равно (без создания подразделения не обойтись)

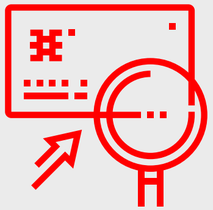
От бумажной ИБ к результативной



Мы не можем защититься от всего и сразу – надо фокусировать на важном. Необходимо определить недопустимые события



Возможность реализации недопустимого события подтверждает в рамках независимого анализа защищенности (пентеста)



Анализ защищенности завершается разработкой мер нейтрализации выявленных способов проникновения, направленных на реализацию недопустимых событий

Вся наша жизнь заключается в выборе между допустимым, нежелательным и недопустимым

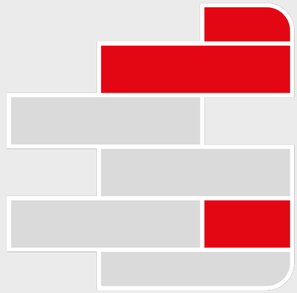
В пределах допустимого

- Превысили скорость на 20 км/ч
- Ушиб от удара футбольного мяча
- Трата 100 рублей городской туалет
- Публикация ПДн в соцсетях

Нежелательно

- Поцарапал автомобиль на стоянке
- Перелом ноги во время футбольного матча
- Потеря кошелька с 10 тысячами рублей
- Утечка адреса доставки пиццы

Недопустимо



- ДТП со смертельным исходом
- Сотрясение мозга с необратимыми последствиями
- Кража 1 миллиона рублей со счета в банке
- Утечка данных кредитной карты, а также медицинских данных

Что такое недопустимое событие?

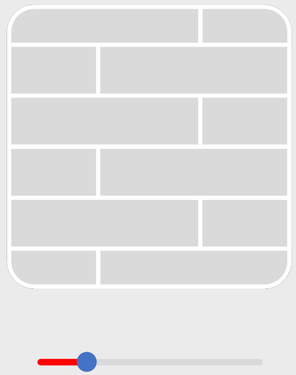
На каждом уровне экономики есть события, которые недопустимы

—события, делающие невозможным достижение предприятием, отраслью, государством операционных и стратегических целей или приводящие к длительному нарушению основной деятельности, в результате кибератак

Воздействие кибератаки на организацию

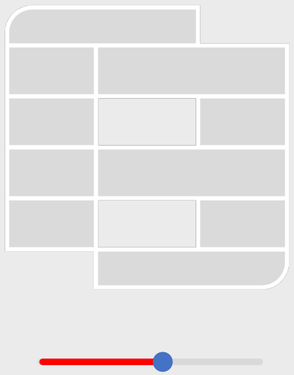
- крупные финансовые потери
- публичные судебные разбирательства
- остановка производственных процессов
- потеря доли рынка
- срыв контрактных обязательств

Выполняет все свои функции



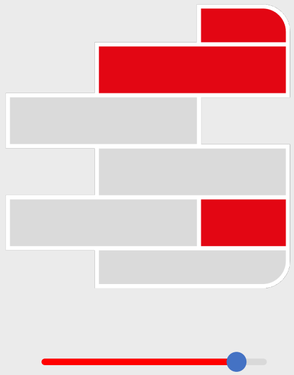
допустимый ущерб

Выполняет свои функции частично



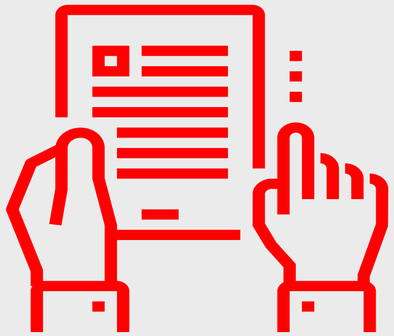
значительный ущерб

Не выполняет свои функции



недопустимый ущерб

Это не новация –
мы с этим уже сталкивались



Ключевые
риски в анализе
рисков

Негативные последствия
в методике оценки угроз
ФСТЭК

Реестр недопустимых событий

НЕДОПУСТИМОЕ СОБЫТИЕ	СЦЕНАРИИ РЕАЛИЗАЦИИ	ЦЕЛЕВЫЕ СИСТЕМЫ	КРИТЕРИИ РЕАЛИЗАЦИИ
Утечка персональных данных более 10 тысяч клиентов компании, повлекшая штраф в размере 4% от оборота	▪ Несанкционированный доступ к серверу баз данных с ПДн ▪ Кража ноутбука с ПДн ▪ Взлом через подрядчика (supply chain attack)	▪ CRM-система ▪ 1С:ERP или SAP ▪ Система управления лояльностью	▪ Доступ к CRM-системе с с привилегиями на копирование данных на внешний носитель ▪ Прямой доступ к базе данных 1С или SAP, минуя доступ через приложение ▪ Доступ к ноутбуку сотрудника отдела продаж ▪ Доступ к резервной копии базы данных при условии отсутствия ее шифрования

Другие примеры недопустимых событий

Непредоставление государственной услуги на 4 часа

За счет ddos-атаки или sql-инъекции или шифрования портала госуслуг или удаления базы пользователей...

Срыв контрактных обязательств по поставке трубопроката на 3 дня

За счет нарушения функционирования технологического процесса или уничтожения системы управления цепочками поставок...

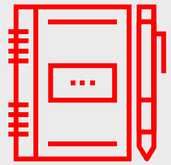
Демонстрация политических лозунгов на телевизионном канале

За счет взлома CDN или стримингового сервиса с последующим перенаправлением на ресурсы оппозиционных СМИ или подмешивание постороннего контента или взлом системы показа рекламы...

Недопуск болельщиков на матч крупного спортивного мероприятия

За счет обнуления базы болельщиков (fanid) или взлома системы контроля доступа на стадион...

Что дальше?

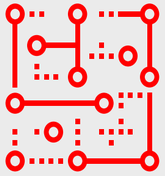


Сбор информации о системах защиты информации и выявление недостатков в них

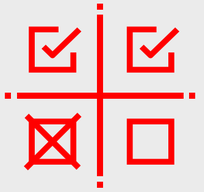
Выявление недостатков в организации и архитектуры ИБ

Независимая оценка уровня защищенности

Разработка перечня мер нейтрализации

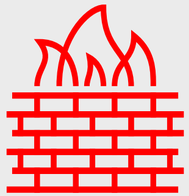


Проверка практической возможности использования недостатков злоумышленниками

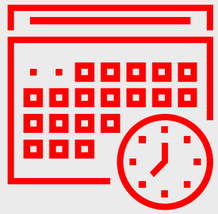


Оценка возможности возникновения недопустимых событий

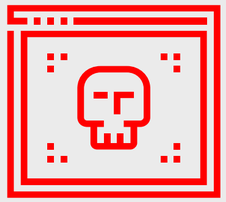
Финальный аккорд 250-го Указа



Все попавшие под Указ организации не смогут закупать и использовать средства защиты из недружественных государств, а также иных организаций, которые прямо или косвенно подконтрольны таким государствам



С 1-го января 2025-го года. Не забывайте также про Указ №166 и планируемое обновление 166-го Указа на всех субъектов КИИ, а не только заказчиков по 223-ФЗ



Список недружественных стран определяет Правительство и он регулярно расширяется, что создает риски для использования любых иностранных решений. И не забывайте про 166-й Указ, который распространяется на любое иностранное ПО, а не только исходящее из недружественных государств

Кто недружественный нам?

Распоряжение Правительства от 5 марта 2022 года №430-р
и распоряжение Правительства от 23 июля 2022 года №2018-р

- Австралия
- Албания
- Андорра
- Багамские о-ва
- Великобритания (включая о. Гернси, о. Джерси и о. Мэн (коронные владения Британской короны) и подконтрольные заморские территории - о. Ангилья, Британские Виргинские острова, Гибралтар)
- Государства - члены Европейского союза
- Исландия
- Канада
- Лихтенштейн
- Микронезия
- Монако
- Новая Зеландия
- Норвегия
- Республика Корея
- Сан-Марино
- Северная Македония
- Сингапур
- Соединенные Штаты Америки
- Тайвань (Китай)
- Украина
- Черногория
- Швейцария
- Япония

250-й Указ – это не все, что нас ждет

- Новые правила аккредитации центров ГосСОПКИ
- Оборотные штрафы за утечку и скрытие факта утечки ПДн, а также уголовная ответственность за утечку и использование незаконно полученных ПДн, в том числе и повлекших тяжелые последствия
- Совместный регламент/приказ РКН и ФСБ по уведомлению об утечках
- Новый Указ Президента по импортозамещению на всех ОКИИ, а не только значимых

alukatsky@ptsecurity.com

ptsecurity.com

Спасибо за внимание

О Positive Technologies

20 лет
исследований и опыта в обеспечении кибербезопасности

300+
экспертов в крупнейшем исследовательском центре в Европе

10 лет
проводим самые крупные в России и Европе киберучения

80%
отечественных компаний рейтинга «Эксперт-400» используют наши продукты и услуги

Positive Technologies уже 20 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира.
В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».
Следите за нами в соцсетях,а также в разделе «Новости» на сайте ptsecurity.com.