

ITSec: Кибербезопасность предприятия и защита инфраструктуры, информационных систем, данных и приложений от современных угроз

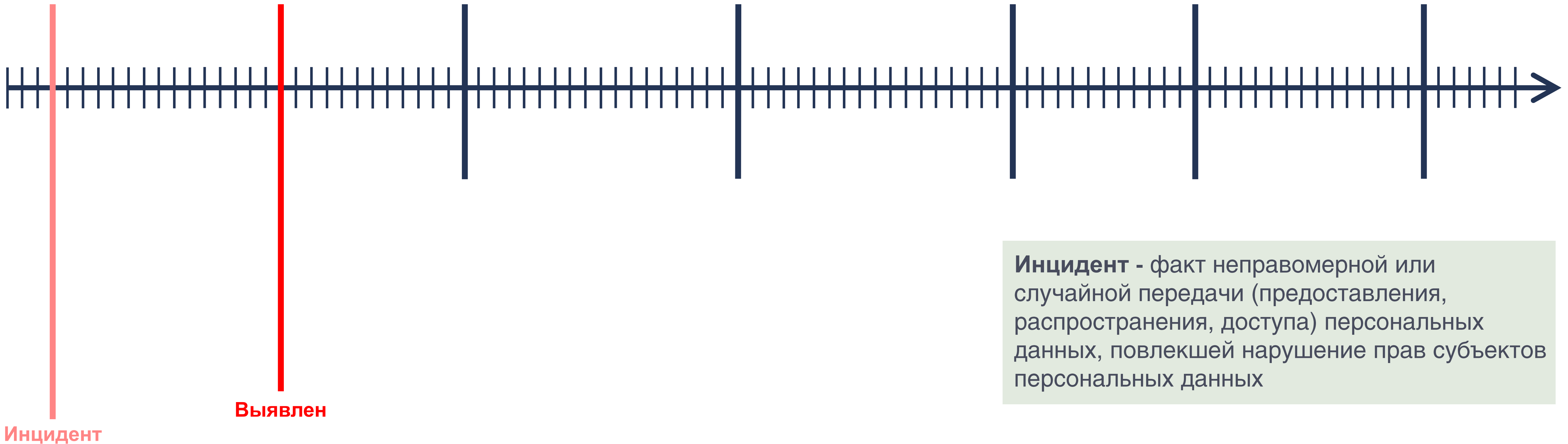
Станислав Румянцев, к.ю.н., CIPP/E
старший юрист

РЕАГИРОВАНИЕ НА УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ: ТОП-5 ЮРИДИЧЕСКИХ СОВЕТОВ

1.

**Определить, когда и о чем
уведомлять Роскомнадзор**

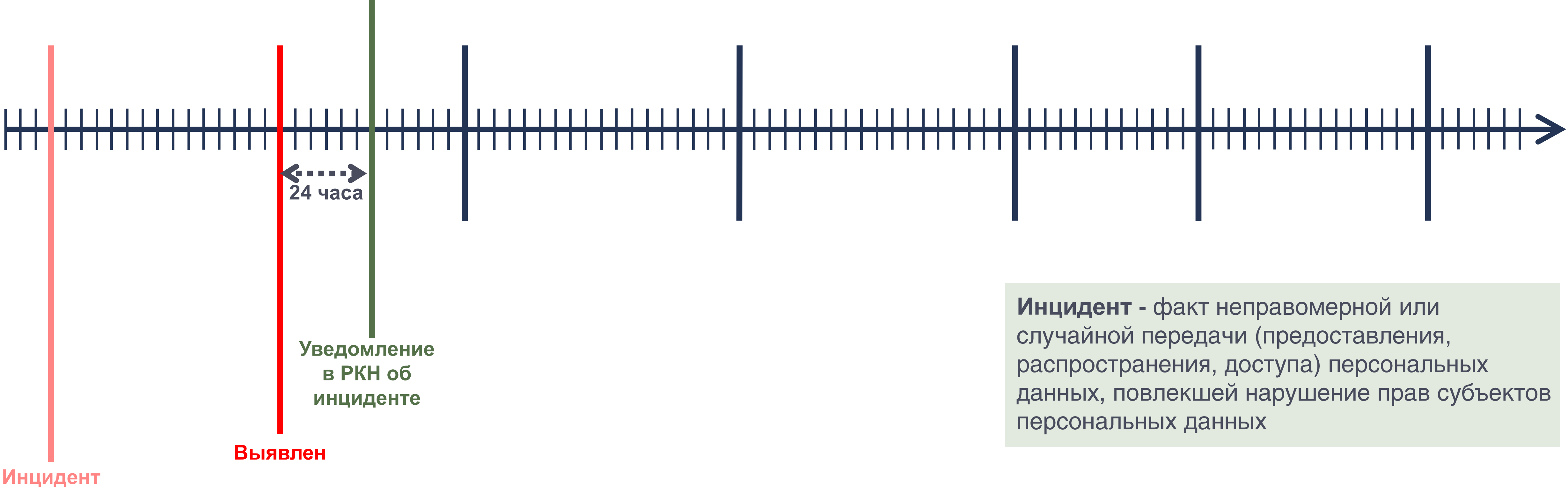
Часть 3.1 ст.21 Федерального закона «О персональных данных»



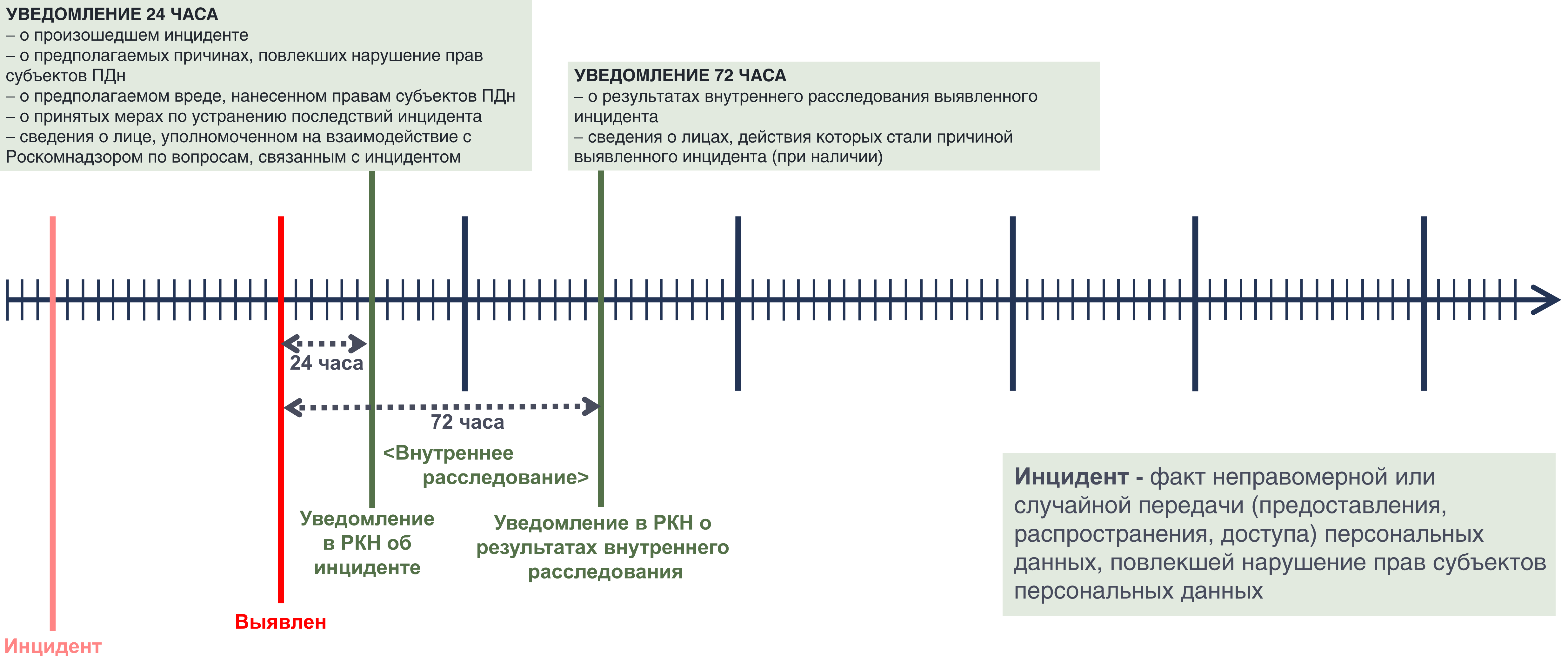
Часть 3.1 ст.21 Федерального закона «О персональных данных»

УВЕДОМЛЕНИЕ

- о произошедшем инциденте
- о предполагаемых причинах, повлекших нарушение прав субъектов ПДн
- о предполагаемом вреде, нанесенном правам субъектов ПДн
- о принятых мерах по устранению последствий инцидента
- сведения о лице, уполномоченном на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом



Часть 3.1 ст.21 Федерального закона «О персональных данных»



2.

Учитывать требования Трудового кодекса

Ответственность работника по Трудовому кодексу

ДИСЦИПЛИНАРНАЯ

пп. в) п.6 ст.81 ТК: Трудовой договор может быть расторгнут работодателем в случаях: <...>

разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Инцидент - факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

ПОЛНАЯ МАТЕРИАЛЬНАЯ

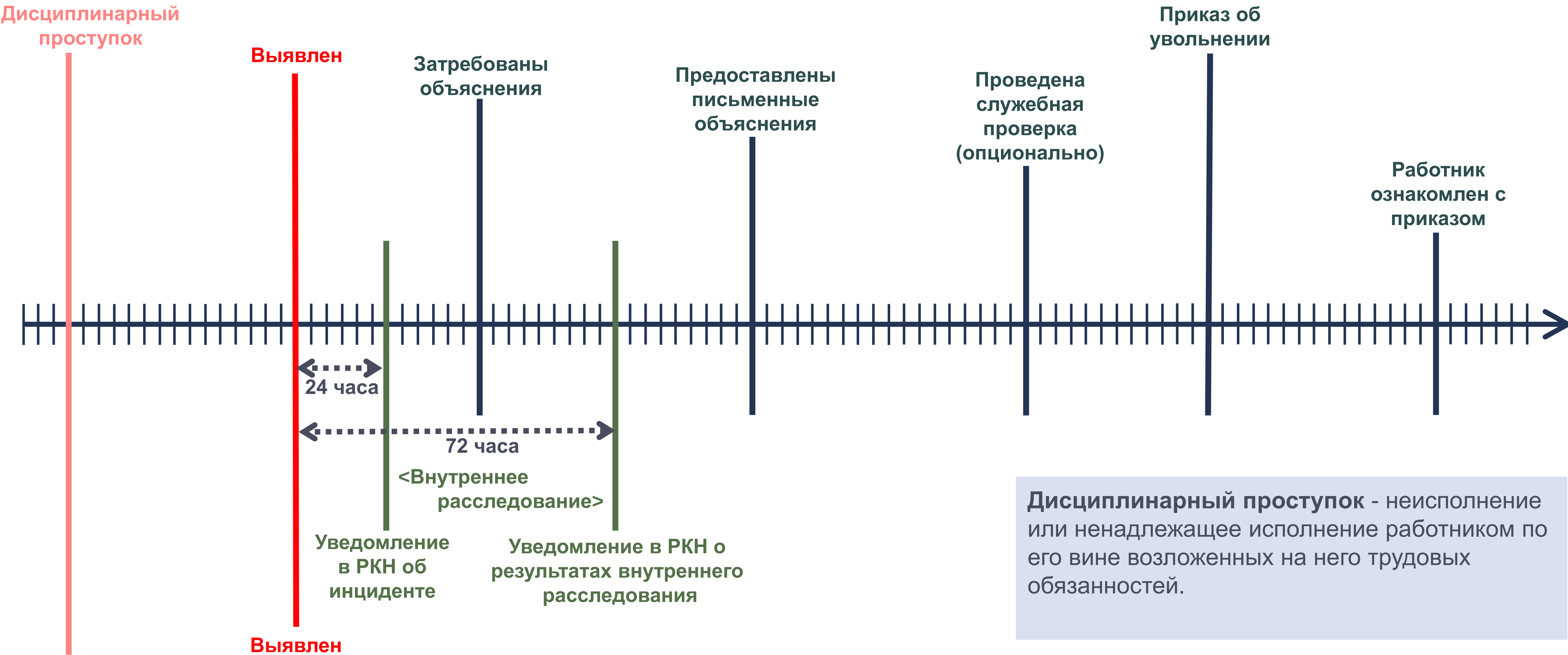
п. 5, 6, 7 ст.243 ТК: Материальная ответственность в полном размере причиненного ущерба возлагается на работника в следующих случаях: <...>

5) причинения ущерба в результате преступных действий работника, установленных приговором суда;

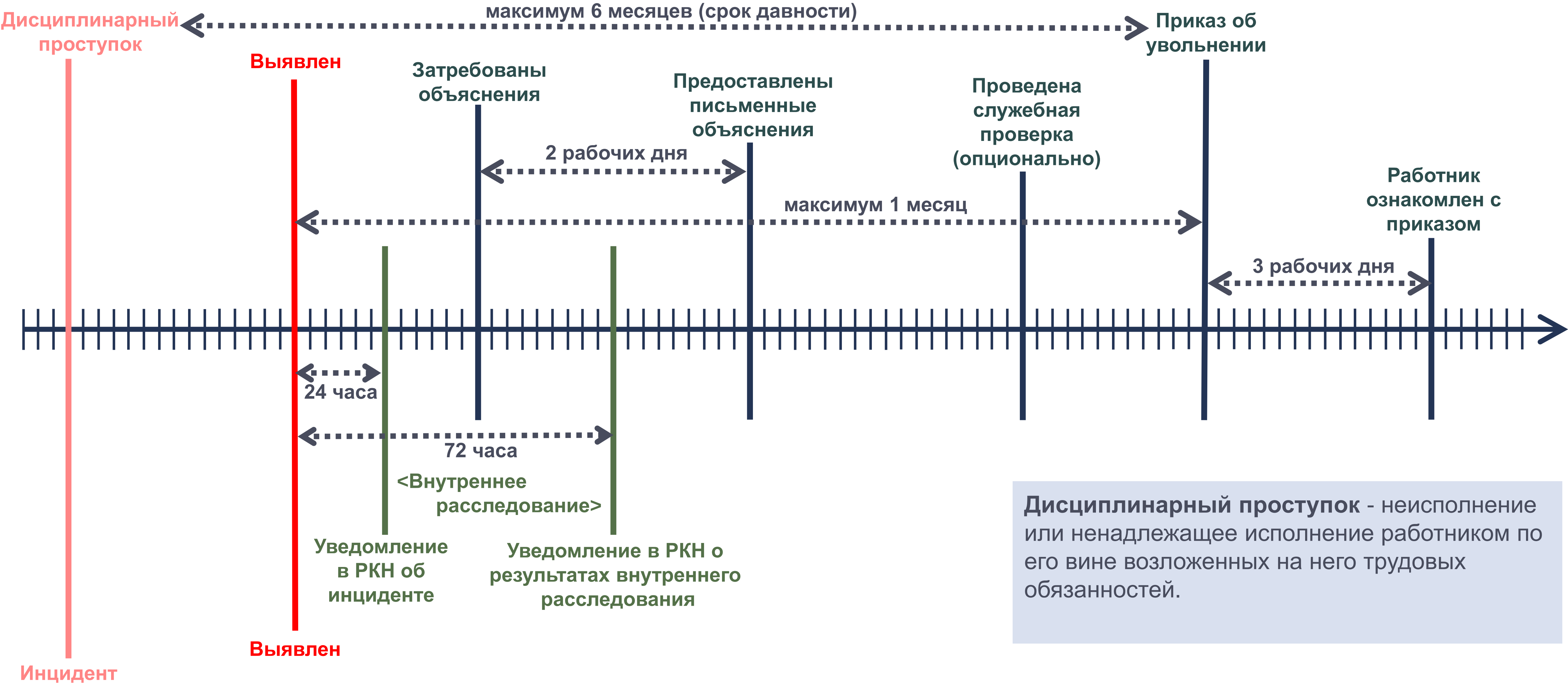
6) причинения ущерба в результате административного правонарушения, если таковое установлено соответствующим государственным органом;

7) разглашения сведений, составляющих охраняемую законом тайну (государственную, служебную, коммерческую или иную), в случаях, предусмотренных настоящим Кодексом, другими федеральными законами.

Статья 193 Трудового кодекса



Статья 193 Трудового кодекса



Дисциплинарный проступок - неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей.

3.

**Правильно установить
обстоятельства в ходе
внутреннего расследования /
проверки**

Какие обстоятельства имеют значение?

Расследование инцидента

- Факт инцидента
- Предполагаемые причины, повлекшие нарушение прав субъектов персональных данных
- Предполагаемый вред, нанесенный правам субъектов персональных данных
- Меры по устранению последствий соответствующего инцидента,
- Сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии)
- Прочее

(ст.21 Федерального закона «О персональных данных»)

Проверка по дисциплинарному проступку

- Факт дисциплинарного проступка
- Тяжесть совершенного проступка
- Обстоятельства, при которых проступок был совершен
- Работник, совершивший дисциплинарный проступок, и его вина
- Предшествующее поведение работника
- Отношение работника к труду
- Сведения, которые работник разгласил относятся к государственной, служебной, коммерческой или иной охраняемой законом тайне, либо к персональным данным другого работника
- Эти сведения стали известны работнику в связи с исполнением им трудовых обязанностей
- Работник обязывался не разглашать такие сведения
- Предприняты достаточные меры по защите конфиденциальной информации
- Прочее

Трудовой кодекс

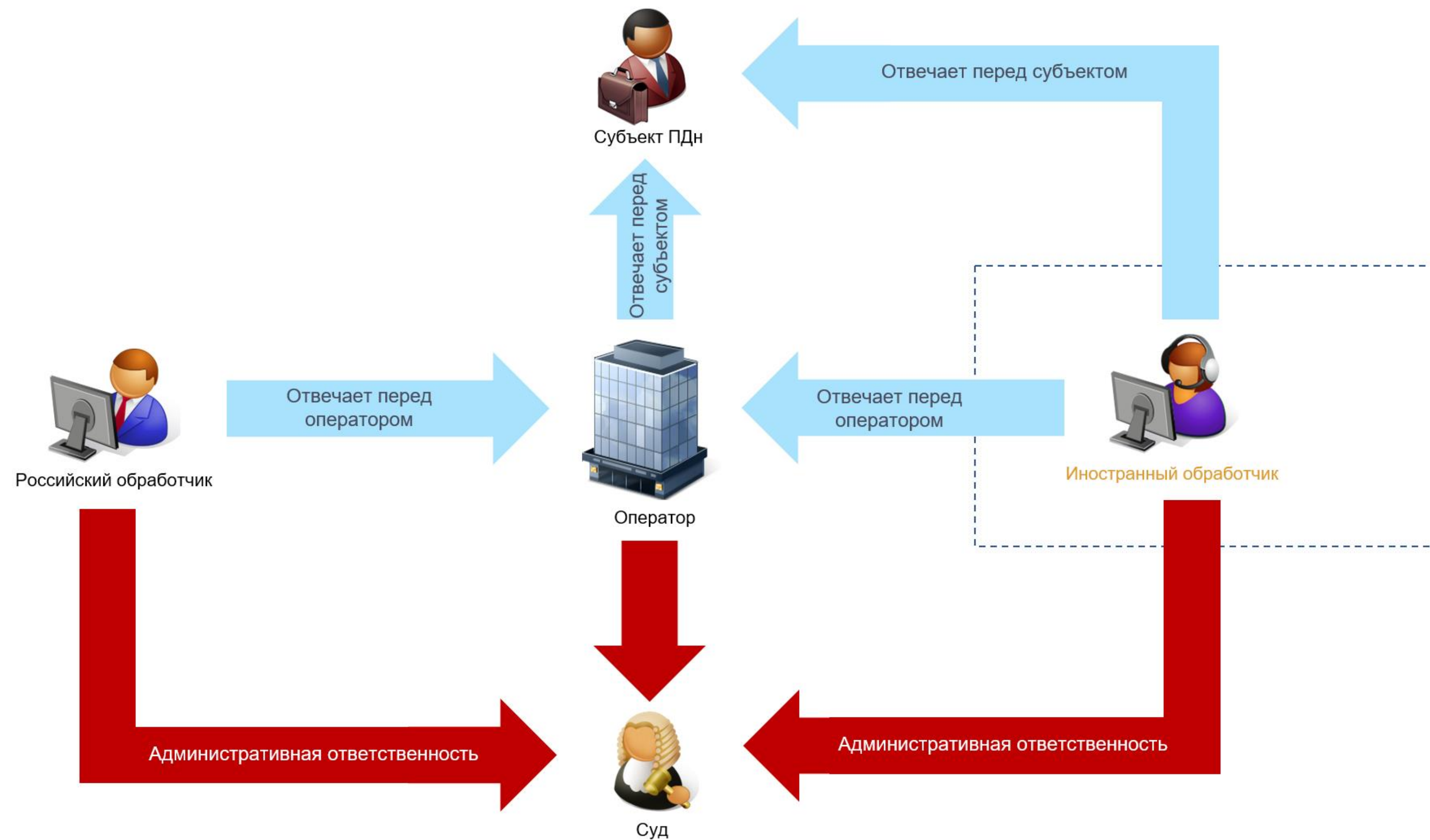
Постановление Пленума ВС РФ
от 17.03.2004 № 2

Постановление
КС РФ
от 26.10.2017
№ 25-П

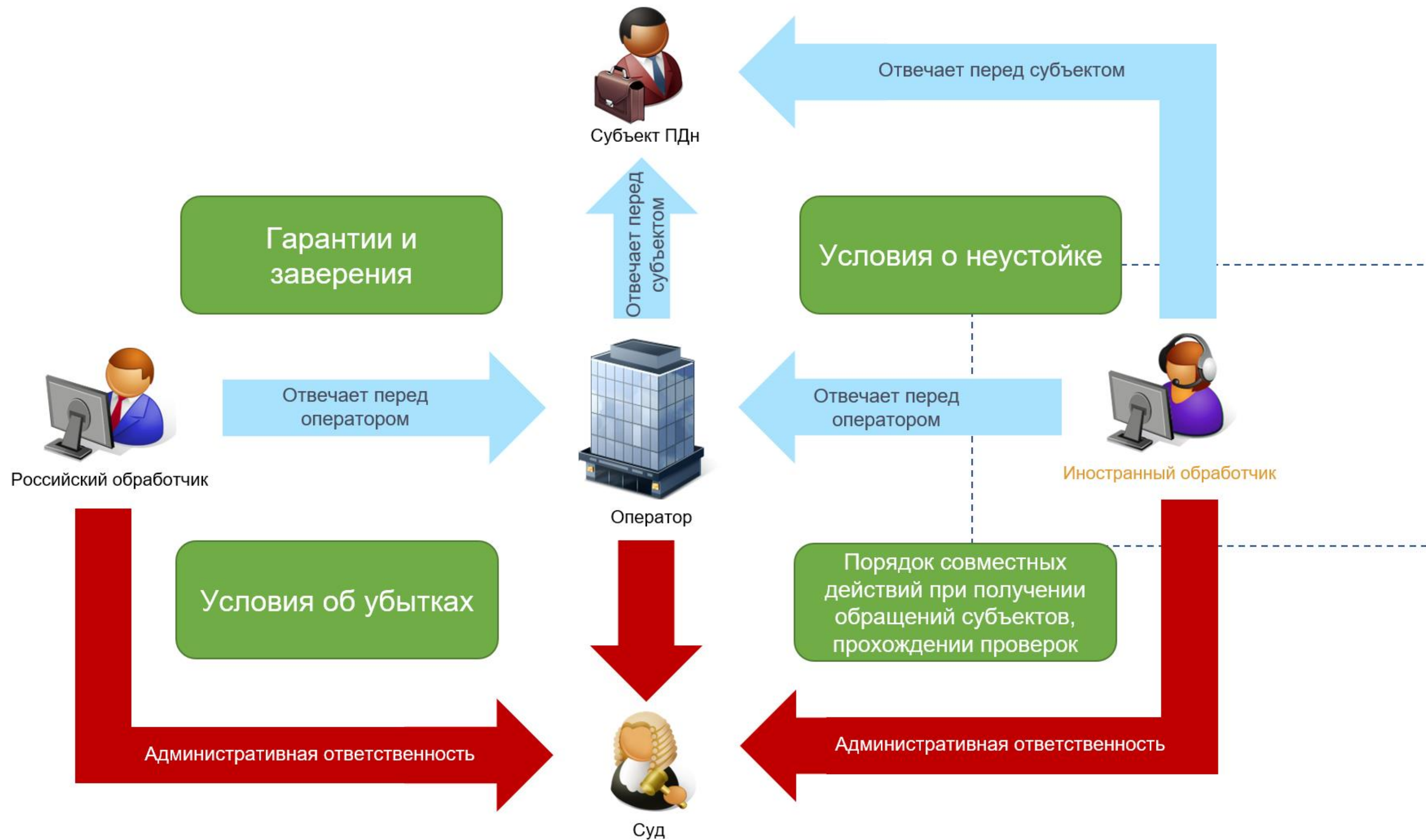
4.

**Включить условия об утечках
в договоры с подрядчиками**

Заранее договориться о порядке совместных действий и ответственности



Заранее договориться о порядке совместных действий и ответственности



5.

УЧИТЫВАТЬ РИСКИ

Основные правовые риски при утечках персональных данных

Предписание

Административные
штрафы

Гражданский иск
от субъектов
персональных данных

Репутационные потери

Выводы

- Процесс реагирования на инциденты необходимо продумать и отразить в локальных нормативных актах заранее. При утечке нужно действовать быстро
- Правила уведомления Роскомнадзора об инциденте и порядок привлечения к дисциплинарной ответственности плохо сочетаются. Надо ставить приоритеты с учетом ситуации и правовых рисков
- Во внутреннем расследовании должны участвовать технические специалисты и юристы. Обстоятельства утечки имеют юридическое значение
- С подрядчиками (лицами, обрабатывающими персональные данные по поручению оператора) необходимо заранее договариваться о порядке действий в случае инцидента. После утечки – дружба и партнерские отношения закончатся
- Оценка правовых рисков – обязательная часть комплаенса в области персональных данных. Она проводится до утечки, а не после

Спасибо за внимание!

Станислав Румянцев
к.ю.н., СІРР/Е
Старший юрист

г. Москва, ул. Большая Спасская, 25, стр.3

RumyantsevS@gorodissky.com

www.gorodissky.ru

© ООО «Юридическая фирма Городисский и партнёры», 2024