SCS SBERBANK CYBER SECURITY

INTERNATIONAL CONFERENCE
PERSONAL DATA PROTECTION

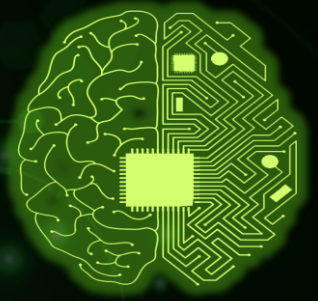
НОВЫЕ ВЫЗОВЫ И УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Евгений Калинин
Исполнительный директор –
начальник Центра организации обработки
и защиты персональных данных ПАО Сбербанк

ЭКОНОМИКА ДАННЫХ

Новые Экосистемы

Большие данные



Машинное обучение

Новые продукты

Повышение эффективности бизнеса

Улучшение качества жизни населения

Персональные данные – основная составляющая цифровизации

в **5** раз
2018 – 2025 увеличение глобального объема данных

92% Компаний-респондентов считают, что данные – это потенциальная ценность*

94% Компаний-респондентов считают, что знания о клиентах критично важны*

93% Респондентов считают, что ПДн должны защищаться не менее надежно, чем банковская тайна*

36% Компаний-респондентов уже монетизируют данные*

*По данным опросов Dell EMC и PWC

НОВЫЕ ТЕХНОЛОГИЧЕСКИЕ РЕАЛИИ

INTERNATIONAL CONFERENCE PERSONAL DATA PROTECTION

SCS SBERBANK CYBER SECURITY

- Пятое поколение мобильной связи
- Облака – частные, публичные, гибридные
- Новые системы хранения
- Чат-боты, умные помощники
- Big Data
- Интернет вещей
- Биометрическая идентификация
- Искусственный интеллект
- Аналитика и точный таргетинг

- Кража личных данных
- Вирусы, способные остановить бизнес
- Открытая продажа информации
- Новые, не всегда протестированные технологии
- Низкий уровень киберкультуры населения
- Легкий доступ к инструментам и «продуктам» взломщиков
- Пренебрежение правами субъекта
- Бюрократия
- Низкий уровень международного взаимодействия

Взрывной рост интереса к технологии неизбежно влечет появление соответствующих угроз

КРУПНЫЕ УТЕЧКИ 2019

INTERNATIONAL CONFERENCE PERSONAL DATA PROTECTION

SCS SBERBANK CYBER SECURITY

ЯНВАРЬ

Фотохостинг 500px

> 14 млн учетных записей пользователей

МАРТ

Утечка у компании-партнера Facebook

540 млн учетных записей пользователей

МАЙ

Национальный университет Австралии

Все ПДн накопленные за 19 лет

ИЮЛЬ

ИБ-компания Imperva

Утечка данных клиентских ключей **API и SSL-сертификатов**

СЕНТЯБРЬ

Adobe Creative Cloud

7,5 млн учетных записей пользователей

Более 2000 подтвержденных фактов утечек данных [1]

ФЕВРАЛЬ

> 14 000 чувствительных записей о здоровье

Сингапур, Министерство Здравоохранения

АПРЕЛЬ

763 млн адресов электронной почты

Verification.io

ИЮНЬ

885 млн транзакций

First American Corp.

АВГУСТ

> 5 млн персональных данных граждан

Болгария, Национальное агентство по доходам

ОКТЯБРЬ

2,5 млн записей о клиентах

Yves Rocher

1 По данным компании Verizon

ОСНОВНЫЕ ПРИЧИНЫ И ПОСЛЕДСТВИЯ УТЕЧЕК

Атака на защищенный информационный периметр

Кража ПДн работниками компании

Использование (передача)
ПДн с нарушением прав субъектов

Моральный вред
Рассылка рекламы и спама

Материальный вред
Кража с банковского счета

Имущественный вред
Мошенничество с недвижимостью

МОШЕННИЧЕСТВО С ДАННЫМИ

INTERNATIONAL CONFERENCE PERSONAL DATA PROTECTION

SCS SBERBANK CYBER SECURITY

ТЕНЕВАЯ ИНДУСТРИЯ

> 90%
социальная инженерия

↑40%
в год

- Принуждение к передаче секретов
- Принуждение к самопереводам
- Навязывание услуг
- Регистрация сервисов на чужое имя
- Подделка документов

>50
преступных групп

ТЕНЕВОЙ РЫНОК ДАННЫХ

↑24%
в год

- Вербовка, предательство
- Фишинг
- Взломы ИТ
- Вирусные атаки
- Перепродажа данных

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Законодательство Российской Федерации

Законодательство Европейского Союза

Ответственное лицо

Ответственный за организацию обработки и защиты ПДн (Data Protection Officer)

Организационные меры

Политика обработки персональных данных

Регламент обработки и защиты персональных данных

Стандарты, методики, технологические схемы, альбомы форм

Технические меры

Реализация требований к обработке и защите ПДн:

- при проектировании архитектуры АС
- при проектировании пилотов, процессов

Защита от НСД
Антивирусная защита
Предотвращение вторжений
Защита от утечек

Межсетевое экранирование
Защита от DDoS
Криптозащита
Защита носителей

Формирование требований. Разработка ВНД
Взаимодействие с Регуляторами
Оценка угроз безопасности
Обеспечение адекватной защиты
Расследование инцидентов
Обработка обращений Субъектов
Уведомление Регуляторов / Субъектов ПДн

Процесс управления обработкой и защитой персональных данных

Ведение реестра процессов
Имплементация требований в процессы
Оценка вреда Субъекту и DPIA
Контроль процессов
Организация взаимодействия с контрагентами
Обработка запросов Регуляторов
Мониторинг законодательства

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

- Коммуникации с клиентами
- Сброс паролей / перевыпуск карт
- Меры по блокировке источника утечки

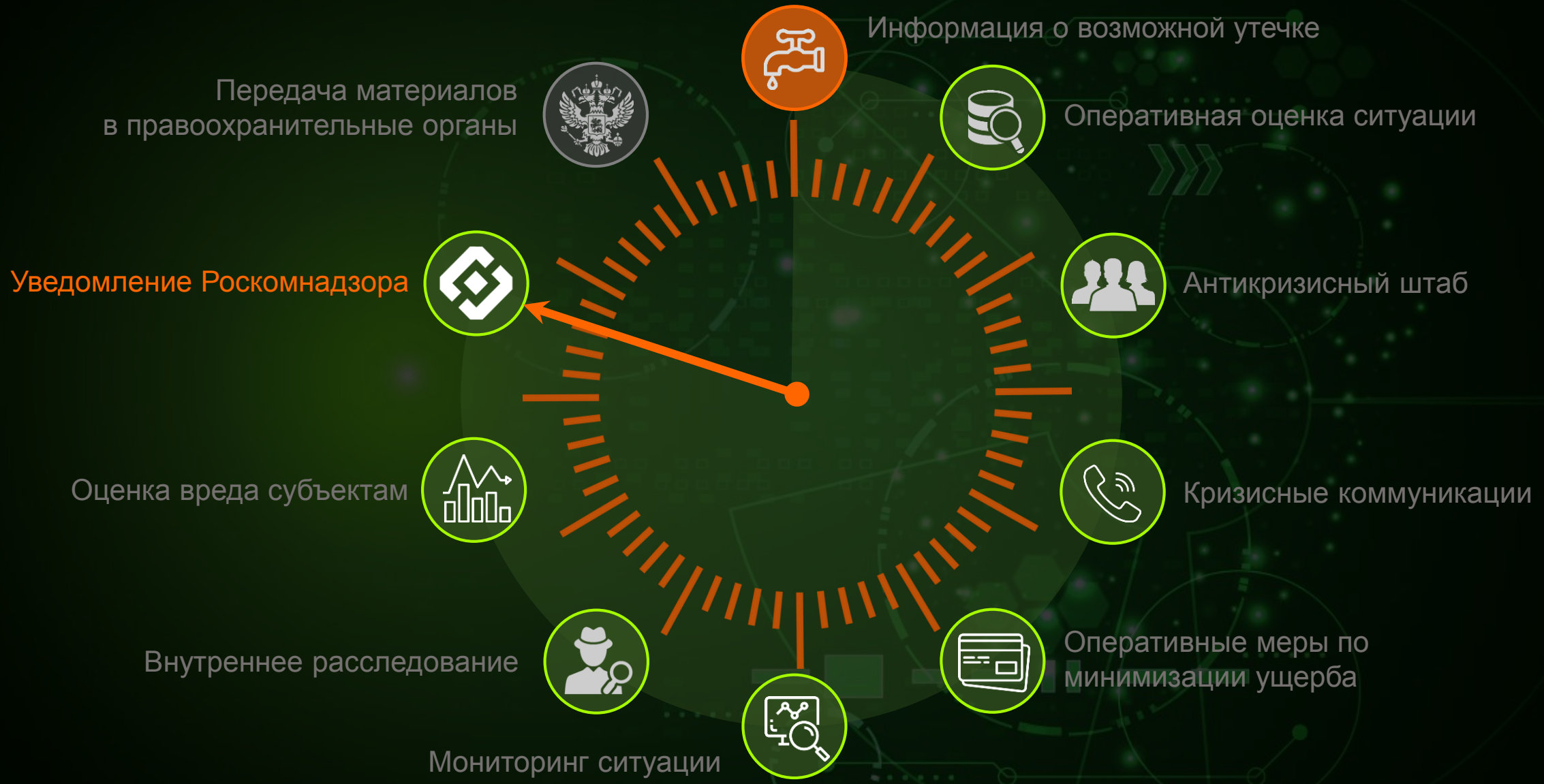
ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

- Функционирование систем
- СМИ и социальные сети
- Управление резервами, логистикой и т.п.

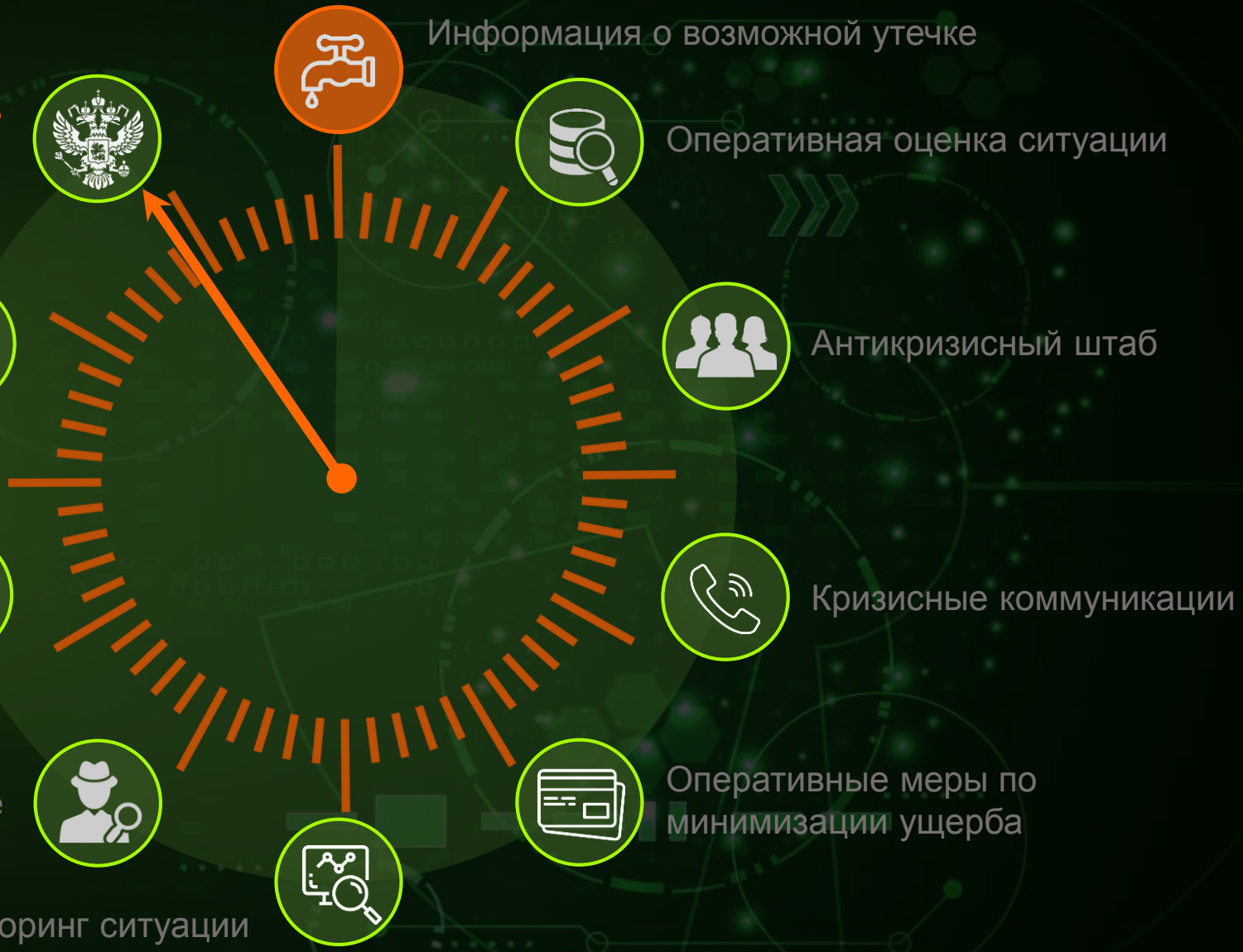
ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

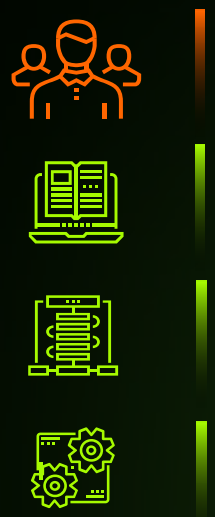


ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?



ЧТО ДЕЛАТЬ ЕСЛИ ПРОИЗОШЛА УТЕЧКА?

ВЫВОДЫ



Кардинально усилить контроль доступа сотрудников к системам, чтобы минимизировать влияние человеческого фактора

КУЛЬТУРА НЕТЕРПИМОСТИ К МОШЕННИЧЕСТВУ

Выделение **КАТЕГОРИЙ СОТРУДНИКОВ** по уровню доступа к персональным данным

РАБОТА по обучению работников, мониторингу и контролю

РЕГУЛЯРНЫЙ КОНТРОЛЬ за мерами, принятыми по фактам нарушений требований безопасности

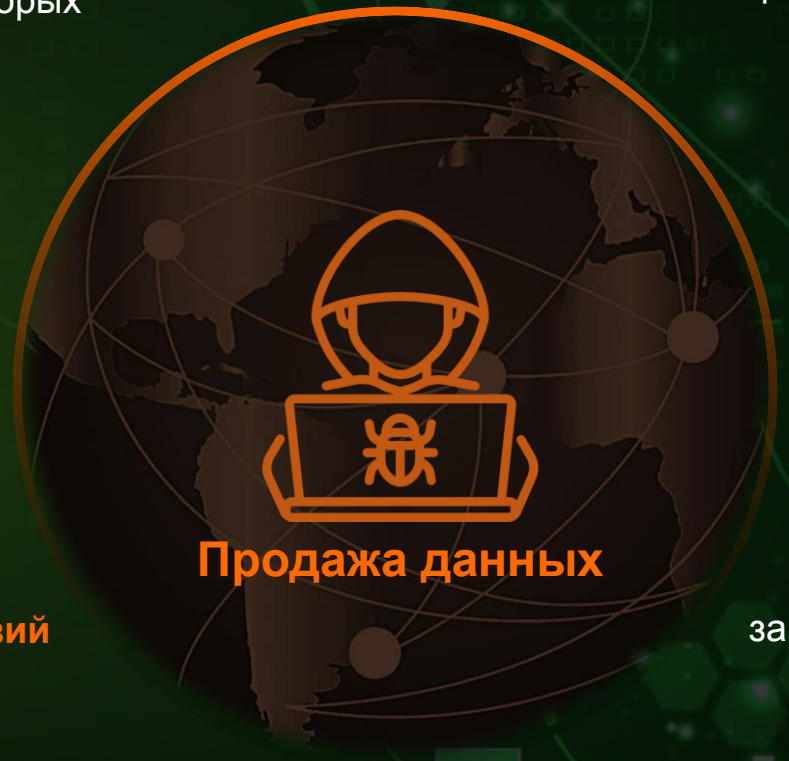
ПРОБЛЕМЫ

INTERNATIONAL CONFERENCE PERSONAL DATA PROTECTION

SCS SBERBANK CYBER SECURITY

Невозможность оперативной блокировки ресурсов, на которых распространяются ПДн

Проблемы законодательства и правоприменительной практики при раскрытии преступлений



Отсутствие скоординированных действий операторов ПДн и госорганов

Либеральность наказания за нарушения в сфере оборота персональных данных

В условиях массовой угрозы для граждан страны

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется усиление уголовной ответственности

183 УК РФ

Продвижение предложений о повышении нижнего порога ответственности за собирание сведений, составляющих КТ, НТ и БТ незаконным способом. Незаконное разглашение и использование этих сведений

Сейчас – 80 тыс. руб.

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется внедрение механизмов оперативной блокировки

Продвижение предложений о блокировке в сети Интернет информации, содержащей сведения о ресурсах, способах покупки/продажи персональных данных и информации, позволяющей осуществлять подмену телефонных номеров, а также о способах и методах такой подмены

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется определить действия ФОИВ и ответственных организаций в экстренных случаях

Продвижение предложений по регламентированию действий ФОИВ и ответственных организаций в экстренных случаях, предполагающих значительный ущерб и угрозу общественной безопасности

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется установление запрета занимать должности, связанные с работой с персональными данными

Продвижение предложений о введении дополнительных квалифицирующих признаков в части установления наказания для нарушителя в виде запрета занимать позиции, связанные с работой с персональными данными, на определенный срок

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется развитие взаимодействия между правоохранительными органами и бизнесом

Продвижение предложений об усилении взаимодействия с правоохранительными органами по вопросам борьбы с преступлениями в отношении защищаемой информации и с фактами мошенничества

ЧТО ДЕЛАТЬ НА УРОВНЕ ГОСУДАРСТВА

Требуется повышение киберкультуры населения

Продвижение предложений по подготовке кадров от уроков компьютерной грамотности в школах, до обновления стандартов образования в ВУЗах

SCS SBERBANK CYBER SECURITY

INTERNATIONAL CONFERENCE
PERSONAL DATA PROTECTION

Спасибо за внимание