ГАРДА

Трек 4

# Строим экосистему по защите данных

Трек 4

# Строим экосистему по защите данных

## Модератор

### Андрей Вишняков

Пресейл-директор, ГК «Гарда»

## Участники

### Вячеслав Касимов

Директор департамента информационной безопасности, Московский кредитный банк

### Дмитрий Соломенцев

Управляющий директор Управления по обеспечению информационной безопасности Департамента по обеспечению безопасности, Банк ВТБ (ПАО)

### Дмитрий Ларин

Директор по разработке продуктов компании "Гарда Технологии"

### Илья Борисов

Директор департамента методологии ИБ, VK

### Александр Кондратенко

Заместитель директора департамента, начальник управления рисками и развития процессов информационной безопасности Росбанка

### Дмитрий Горлянский

Руководитель отдела технической поддержки продаж компании "Гарда Технологии"

# Защита данных, разберёмся в определениях

## Обеспечение конфиденциальности и приватности

**/1.** **Конфиденциальность** (confidentiality) – это требование не разглашать информацию третьим лицам

**/2.** **Приватность** (privacy) – это право на неприкосновенность частной жизни и личной информации.

Указом президента РФ № 188 определен «Перечень сведений конфиденциального характера», куда входят коммерческая тайна и персональные данные физического лица.

- Построение режима коммерческой тайны осуществляется в соответствии с требованиями ФЗ-98 «О коммерческой тайне».
- Отношения, связанные с обработкой персональных данных, регулируются ФЗ-152 "О персональных данных».

Термин «приватность» не описан в законодательстве РФ, однако концепция отражена в:

- Конституции РФ, которая защищает право на неприкосновенность частной жизни, личную и семейную тайну (ст. 23), право на неприкосновенность жилища (ст. 25).
- законодательстве о персональных данных, которое гарантирует право физического лица контролировать информацию о себе, а также защиту его личной информации (Закон № 152-ФЗ «О персональных данных»).
- законодательстве о врачебной тайне (ст. 13 Закона №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации») или тайне усыновления (ст. 139 Семейного кодекса РФ).

# Защита данных, так о чем мы говорим?

> Безопасность данных – защита от внешних атак и злонамеренных сотрудников, в то время как приватность данных касается вопроса, как данные собираются, используются и ими делятся.

## Взгляд на защиту данных по стороны Storage Networking Industry Association (SNIA)

*В ходе дальнейшего обсуждения здесь будем понимать под защитой данных – приватность данных*

## Защита данных

| Инфраструктурная защита | | | Безопасность данных | | | Приватность | | |
|---|---|---|---|---|---|---|---|---|
| Backup/ Restore | RAID & Erasure Coding | Replication | Encryption | Threat Monitoring | Authentication | Legislation | Policies | Best Practice |
| Archiving | Physical Infrastructure | Data Retention | Access Control | Breach Access And recovery | Data Loss Prevention | 3rd party contacts | Data Governance | Global variations |

**Своевременная Доступность Актуальных Данных**

https://www.snia.org/education/what-is-data-privacy

# Взгляд Gartner на обеспечение приватности данных

ГАРАД

*Beyond GDPR: Five Technologies to Borrow from Security to Operationalize Privacy* (May 6, 2019)

Необходим функционал обнаружения, сопоставления рисков, классификации, контроля доступа, анонимизации и управления жизненным циклом данных.

Интегрированная система управления рисками (**IRM**) определяет требования к защите. Четыре другие - cloud access security broker (**CASB**), data-centric audit and protection (**DCAP**), data loss prevention (**DLP**) and file analysis (**FA**) – формируют экосистему защиты данных.

**Gartner предлагает внедрять приватность данных тремя стадиями:**

☑ **Установка**, где идентифицируются и классифицируются приватные данные, оцениваются риски, формируется операционная среда обработки данных;

☑ **Поддержка**, где расширяется масштаб операций, автоматизируются процессы, накапливается статистика, обогащается информация об инцидентах и пополняются внутренние базы знаний;

☑ **Эволюция**, минимизация рисков без ограничений стандартных операций с данными.

**Establish**

- Discovery
- Classification
- Risk Assessment and Tracking
- Record Keeping (RoPA)
- Data Minimization

**Maintain**

- Measurement and Reporting
- Data Mapping/Life Cycle Visualization
- Privacy Impact Assessment (PIA) Automation

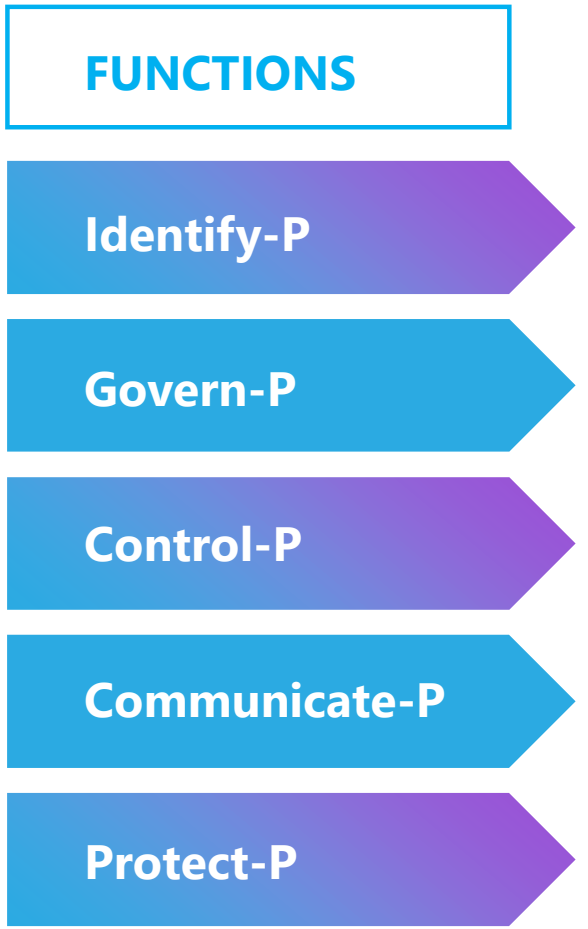
**Evolve**

- Tokenization (Anonymization/ Pseudonymization)
- Business Intelligence and Analytics
- Data End-of-Life Controls

# National Institute of Standards and Technology (NIST)

## Методика защиты приватных данных (Privacy Framework)

- **Идентификация:** определение рисков приватных данных, возникающих при их обработке в организации;
- **Управление:** разработка и внедрение структуры компании, политик, сосредоточенных на управлении рисками приватности данных. Соответствие требованиям регуляторов;
- **Контроль:** разработка и внедрение набора процедур отслеживания, классификации и управления данными, циркулирующими в организации. Внедрение контроля – кто может (и кто должен) иметь доступ к персональным и конфиденциальным данных, полная видимость данных внутри организации.
- **Коммуникация:** организация, персонал и клиенты разделяют понимание, какие данные собираются, как они обрабатываются, и с какими рисками это сопряжено. Прозрачность и в случае компрометации данных.
- **Защита:** внедрение необходимых механизмов защиты персональных и конфиденциальных данных, включая идентификацию и управление рисками, а также разработку стратегии ответных действий, минимизации ущерба в случае утечек данных, кибератак.



# Российский подход

## Меры по защите конфиденциальной информации и персональных данных согласно ФЗ-98 и ФЗ-152

### Охрана конфиденциальности информации (*очень общие формулировки*)

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации;

4) регулирование отношений по использованию информации работниками и контрагентами;

5) нанесение на материальные носители грифа "Коммерческая тайна"

### Обеспечение безопасности персональных данных достигается

1) определением угроз безопасности;

2) применением организационных и технических мер по обеспечению безопасности;

4) оценкой эффективности принимаемых мер по обеспечению безопасности;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных;

8) установлением правил доступа к персональным данным, а также обеспечением регистрации и учета всех действий;

9) контролем за принимаемыми мерами по обеспечению безопасности

# Единая экосистема защиты данных

## Цикл жизни данных

**Хранение**

Файловые хранилища, базы данных, АРМ

**Доступ**

Файловые хранилища, базы данных

**Обработка**

АРМ, сервера приложений, смежные системы

**Передача**

АРМ, смежные системы

На каждом этапе жизненного цикла данных своя модель угроз, соответственно требуются специализированные технологии защиты

# Единая экосистема защиты данных

## Меры защиты

- **Категоризация информации –** файловые хранилища, БД;
- **Мониторинг правил хранения данных –** файловые хранилища, БД, АРМ;
- **Аудит прав доступа -** файловые хранилища, БД;
- **Аудит обращений к хранимым данным –** файловые хранилища, БД, АРМ;
- **Мониторинг действий пользователей при обработке данных –** АРМ;
- **Контроль передачи данных за периметр –** АРМ;
- **Хранение данных аудита для проведения расследований**
- **Агрегация результатов аудита и анализ**

# Защита данных на 360

## Решения

# Защита данных на 360

## Примеры

### DCAP

- Покажет где на ФС хранится критическая информация, кто к ней имеет доступ
- Выявит нарушение правил хранения критических данных при появлении таких файлов в общем доступе
- Покажет историю файла – кто его создали, скопировал, изменял, включая все копии файла

### DBF

- Выявит несанкционированные запросы к критическим данным
- Обнаружит аномально большие выгрузки данных пользователем из БД
- Позволит выявить мошеннические действия с использованием прямого доступа к БД

### DLP

- Выявит факты хранения на АРМ файлов с конфиденциальной информацией, которых там быть не должно
- Предотвратит передачу конфиденциальной информации за периметр
- Выявит факты подделки данных с использованием графических редакторов и других средств

### Data Masking

- Позволит передавать копии БД для разработчиков и тестеров в незащищенные сегменты

# Защита данных на 360

## Работа экосистемы

Довольно часто инцидент представляет собой не единичное действие, а цепочку событий.

Для обнаружения таких инцидентов необходима совместная работа всех средств защиты и корреляция событий

**DCAP**

Копирование файлов с договорами по VIP-клиентам

**DBF**

Запрос данных о состоянии счетов, последних поступлениях денежных средств, локаций, где были проведены последние операции с картой

**DLP**

Выгрузка запароленного архива на внешний носитель

Продажа данных о ВИП клиентах криминальным структурам для последующего **хищения средств**

GARDA

**Офис в Москве**
улица Новодмитровская, дом 2Б
+7 (495) 540 05 27

**garda.ai**
hello@garda.ai