



# Информационная безопасность в цифровой экономике

*ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЦИФРОВОЙ ЭКОНОМИКЕ*

*ЛЕКЦИЯ 5*

к.т.н., доцент  
Буряченко Владимир Викторович

СибГУ им. М.Ф. Решетнева, 2019

## 2

# Цифровая экономика



- В настоящее время происходит формирование цифровой экономики, основанной на разработке и **внедрении современных цифровых технологий в деятельность населения и организаций.**
- Совершенствование анализа **больших данных**, широкое использование **мобильных устройств**, развитие **Интернета**, появление **Интернета вещей**, безусловно являются инновационными элементами, призванными решать социально-экономические проблемы, как на уровне отдельных регионов и стран, так и на мировом уровне.
- Ускорение и усложнение процессов, происходящих в современных условиях развития цифровых технологий, заставляет субъектов экономической деятельности задумываться об **информационной безопасности.**



## Информационные риски цифровой экономики

- Потеря доверия со стороны контрагентов является крайне нежелательным результатом деятельности, поэтому вопросы обеспечения информационной безопасности требуют решения, как на государственном уровне, так и на уровне отдельных организаций.
- Информационные атаки могут иметь мировой масштаб: в мае 2017 г. компьютеры в более чем 150 странах были заражены вирусной программой **WannaCry**.





## Создание безопасной информационной среды

- В условиях высокой цифровой взаимозависимости между различными субъектами экономики создание безопасной информационной среды становится неотъемлемым элементом формирования устойчивой цифровой экономики.
- С точки зрения обеспечения информационной безопасности, наименее контролируемые направления среди множества цифровых технологий являются большие данные, Интернет вещей и технологии искусственного интеллекта.



5

## Проблемы информационной безопасности



- Обеспокоенность последствиями потери личной информации связана с наличием случаев кражи данных, прямо или косвенно связанных с цифровыми технологиями.
- Значительная часть инцидентов связана с нарушением политики конфиденциальности, целостности и доступности информации.

6

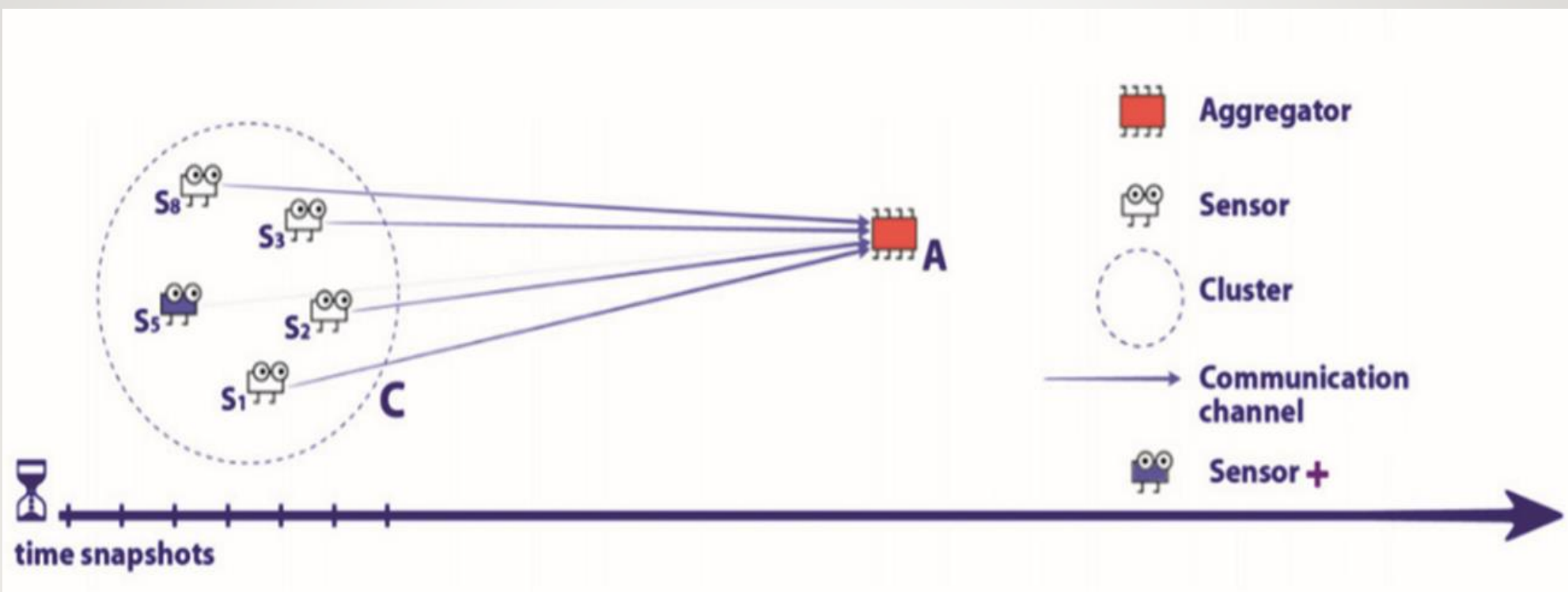
## Киберфизические системы



- В основу технических решений в цифровой экономике положены понятия «**киберфизические системы**» и «**Интернет вещей**».
- Стандарты института NIST (National Institute of Standards and Technology, США) разделяют понятие Интернет вещей на два **IoT** и **NoT** (**Интернет вещей и Сеть вещей**)), которые одинаковы по структуре, но отличаются способом подключения к телекоммуникационным каналам связи:
  - в первом случае (IoT) сенсоры подключены к Интернет.
  - во втором случае (NoT) они находятся внутри локальной сети.

7

## Примитив Network of Things в концепции стандарта



8

## Реализация КФС в рамках модели цифровой экономики



- В качестве примера реализации цифровой экономики приведем следующий. При обмене мнениями с коллегами на Международной научной школе в СПИИРАН РАН по безопасности КФСЗ был приведен пример внедрения новых информационных технологий в медицину в Норвегии.
- Для людей с повышенным риском инфарктов и инсультов в Норвегии разработан браслет, способный контролировать состояние человека и при критичных значениях параметров передавать их и показатели геолокации больного по беспроводной системе связи в центр обработки данных (ЦОД).
- В ЦОД прогнозируется состояние больного и при необходимости его срочной госпитализации автоматически формируется сообщение на мобильный телефон с указанием ближайшего пункта госпитализации.



## 9 | Направление «Информационная безопасность» в цифровой экономике»



- Целью этого направления является достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики.

10

## Направление «Информационная безопасность» в цифровой экономике»



Для реализации этой цели в программе выделено 14 задач и 175 вех.

1. Обеспечить технологическую независимость и безопасность функционирования аппаратных средств и инфраструктуры обработки данных.
2. Обеспечить безопасность функционирования российского сегмента сети Интернет.
3. Разработать нормативно-правовые механизмы функционирования КФС в условиях цифровой экономики (пп.5.5-5.8, 5.10-5.12).
4. Создать основы для построения доверенной среды функционирования КФС.
5. Обеспечить устойчивость и безопасность функционирования информационных систем и технологий (п.5.4 программы).
6. Обеспечить международное взаимодействие по вопросам информационной безопасности в цифровой экономике.



## Сложности при реализации программы

- Наиболее сложной стратегической задачей является первая, направленная на создание технологической независимости отечественного производства аппаратных средств в сфере защиты информации.

## 12

# Оценка уровня информационной безопасности организации



В современных условиях цифровой экономики каждая организация должна регулярно оценивать уровень своей информационной безопасности, отвечая на следующие вопросы:

1. Насколько рационально распределены финансовые ресурсы между кадровым обеспечением организации и цифровыми технологиями, направленными на защиту данных?
2. Правильно ли оценивается важность тех или иных мероприятий по обеспечению информационной безопасности?
3. Созданы ли в организации условия для внедрения современных цифровых технологий по защите информации?
4. Насколько рационально обеспечивается информационная безопасность на всей цепочке оказания услуг или выполнения работ?
5. Эффективно ли менеджмент организации справляется с задачами по обеспечению информационной безопасности?



# 13

## Этапы анализа информационной безопасности организации



- Повышение информационной безопасности организаций может быть обеспечено через проведение многоступенчатого анализа возникающих угроз:

### Этап 1: Инициация анализа

- Обнаружение проблемы
- Частичное решение
- Отсутствие коммуникации и стандартизации

### Этап 2: Управление процессами

- Отслеживание процессов
- Определение ответственностей
- Определение правил выполнения процедур
- Обзоры итогов процессов

### Этап 3: Реализация и контроль

- Контролируемый процесс
- Процедуры коммуникации
- Сбор данных об эффективности
- Интеграция с другими процессами
- Контроль за соблюдением

### Этап 4: Прогнозирование

- Определены потребности корректировки принятых мер
- Постоянное совершенствование
- Инструменты автоматизации
- Связь с бизнес-целями организации

### Этап 5: Оптимизация

- Непрерывное совершенствование
- Интеграция с ИТ
- Полностью автоматизированный процесс защиты данных
- Интеграция во все направления деятельности
- Улучшения на основе новых технологий

## Этапы анализа информационной безопасности организации



- **Этап 1: инициация анализа.** На данном этапе на основе анализа возникающих информационных угроз определяется потребность в пересмотре принятых в организации способов обеспечения сохранности данных.
- **Этап 2: управление процессами.** Обеспечение информационной безопасности разделяется на отдельные процессы, распределяется ответственность за каждый из них.
- **Этап 3: реализация и контроль.** Процесс обеспечения информационной безопасности интегрируется в бизнес-модель, согласуется со стратегией развития организации, проводится контроль за выполнением принятых мероприятий, оценивается результативность нововведений.
- **Этап 4: прогнозирование.** Определение потребности в корректировке принятых мер по обеспечению информационной безопасности, дальнейшее внедрение цифровых технологий с целью более полного охвата возможных угроз.
- **Этап 5: оптимизация.** Проводится непрерывное совершенствование системы обеспечения информационной безопасности; защита данных становится полностью автоматизированным процессом, интегрированным во все направления деятельности организации.

## Государственное регулирование вопросов защиты информации



- В условиях формирования цифровой экономики вопросы защиты информации должны рассматриваться не только на уровне отдельных организаций, но и на государственном уровне.

Программа должна включать ряд этапов:

1. Формирование группы экспертов.
2. Формирование стратегии информационной безопасности.
3. Совершенствование нормативно-правового обеспечения.
4. Разработка современных правовых норм, охватывающих новые отрасли и случаи, не охваченные существующими законами.
5. Разработка и утверждение отраслевых стандартов обеспечения информационной безопасности.
6. Связь процессов информационной безопасности с областью образования.

16

## Вопросы безопасности в рамках развития цифровой экономики



- Цифровая трансформация, проводимая во многих отраслях экономики, привела к тому, что изменился масштаб деятельности экономических субъектов и появились новые риски и угрозы.
- В настоящее время атаки на системы хранения данных становятся всё более сложным и частым явлением, поэтому вопросы обеспечения информационной безопасности должны выступать приоритетной задачей поддержания устойчивости экономики.





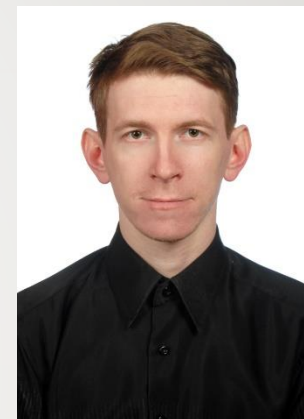
## Список литературы

- Минзов, А. С. Информационная безопасность в цифровой экономике [Электронный ресурс] / Анатолий Степанович Минзов, Александр Юрьевич Невский, Олег Юрьевич Баронов // ИТНОУ: информационные технологии в науке, образовании и управлении. - 2018. - № 3 (7). - С. 52-59. – Режим доступа: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-tsifrovoy-ekonomike>
- TAdviser Статья: Информационная безопасность цифровой экономики России [Электронный ресурс] / Режим доступа: [http://www.tadviser.ru/index.php/Статья:Информационная\\_безопасность\\_цифровой\\_экономики\\_России](http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_цифровой_экономики_России)
- Асаул В.В. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ / Асаул В.В., Михайлова А.О. // Теория и практика сервиса: экономика, социальная сфера, технологии Режим доступа: <https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-usloviyah-formirovaniya-tsifrovoy-ekonomiki> с. 5-9



19

# Информационная безопасность в цифровой экономике



к.т.н., доцент, доцент каф. ИВТ  
Буряченко Владимир Викторович  
Кафедра ИВТ, Л304  
BuryachenkoVV@gmail.com

СибГУ им. М.Ф. Решетнева, 2024