Кибербезопасность в МФЦ

КАСПИЙСК

11 октября, 2018

Кибербезопасность в МФЦ

Цифровая экономика

Цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг

Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»

Кибербезопасность в МФЦ

Риски цифровой экономики

- Маргинализм
- Киберугрозы
- Рост безработицы
- Черная занятость

Целью направления информационной безопасности является достижение состояния **защищенности личности**, общества и государства от **внутренних и внешних информационных угроз**. При таком состоянии будет обеспечиваться реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни, а также суверенитет и устойчивое социально-экономическое развитие России в условиях цифровой экономики.

Кибербезопасность в МФЦ

Нормативное регулирование

- Федеральный закон от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ"О персональных данных"
- Постановление Правительства РФ от 22.12.2012 N 1376 «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг»
- **Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ**

Кибербезопасность в МФЦ

Нормативное регулирование

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

Определяет 13 сфер и областей субъекта КИИ

Области предоставления и оказания государственных и муниципальных услуг нет

Постановление Правительства РФ от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования.. "

Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)

АИС МФЦ формально не относится к КИИ, но при этом выполняет процессы относящиеся к категории социально значимым

Кибербезопасность в МФЦ

Киберландшафт 2018 - злоумышленники

- **Массовые** атаки (WannaCry, BadRabbit, оборудование CISCO, notPetya)
- **Вершина** айсберга:
  - Cobalt Strike, Dimnie, Silence и более 50 других киберпреступных групп
  - 13 новых атакующих инструментов в месяц
  - 2 -3 новые типа атаки в месяц
- Под атакой – **все**

Эксперты: атака с помощью уязвимости Cisco нацелена на информационную инфраструктуру РФ

Интенсивность атак возрастала в 20-30 раз в случае, если была направлена на объекты критической инфраструктуры России

Кибербезопасность в МФЦ

Статистика центра мониторинга безопасности Ростелекома

Средний суточный поток обрабатываемых событий ИБ

1 квартал	2 квартал
9,2 млрд	18,8 млрд

* Динамика – рост на 104%

Доля критичных инцидентов

1 квартал	2 квартал
17,2%	19,4%

Распределение общего количества инцидентов - в дневное время

1 квартал	2 квартал
89,2%	88,1%

Количество событий с подозрением на инцидент, обработанных JSOC

1 квартал	2 квартал
138 256	219 450

* Динамика – рост на 59%

Распределение инцидентов по внешнему/внутреннему вектору атаки

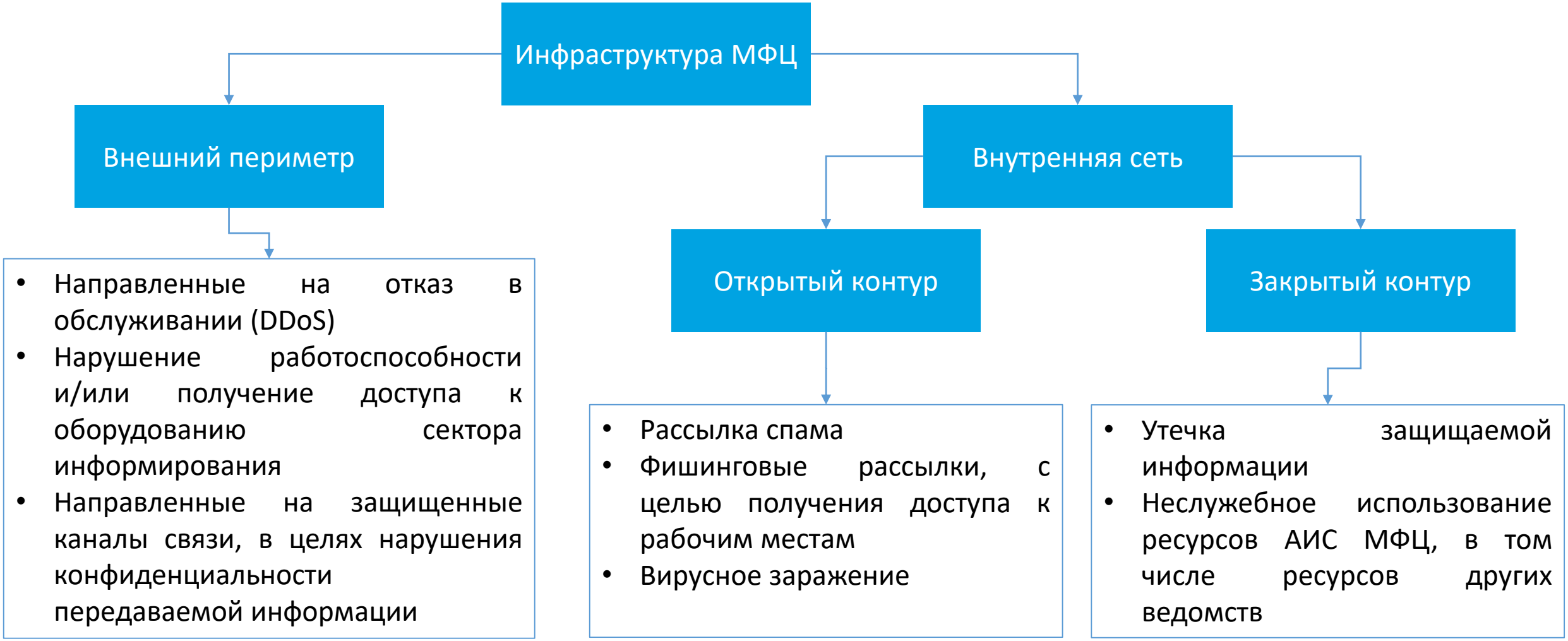
1 квартал	2 квартал
50,3%/49,7%	52,2%/47,8%

Распределение критичных инцидентов в дневное время

1 квартал	2 квартал
72,1%	69,5%

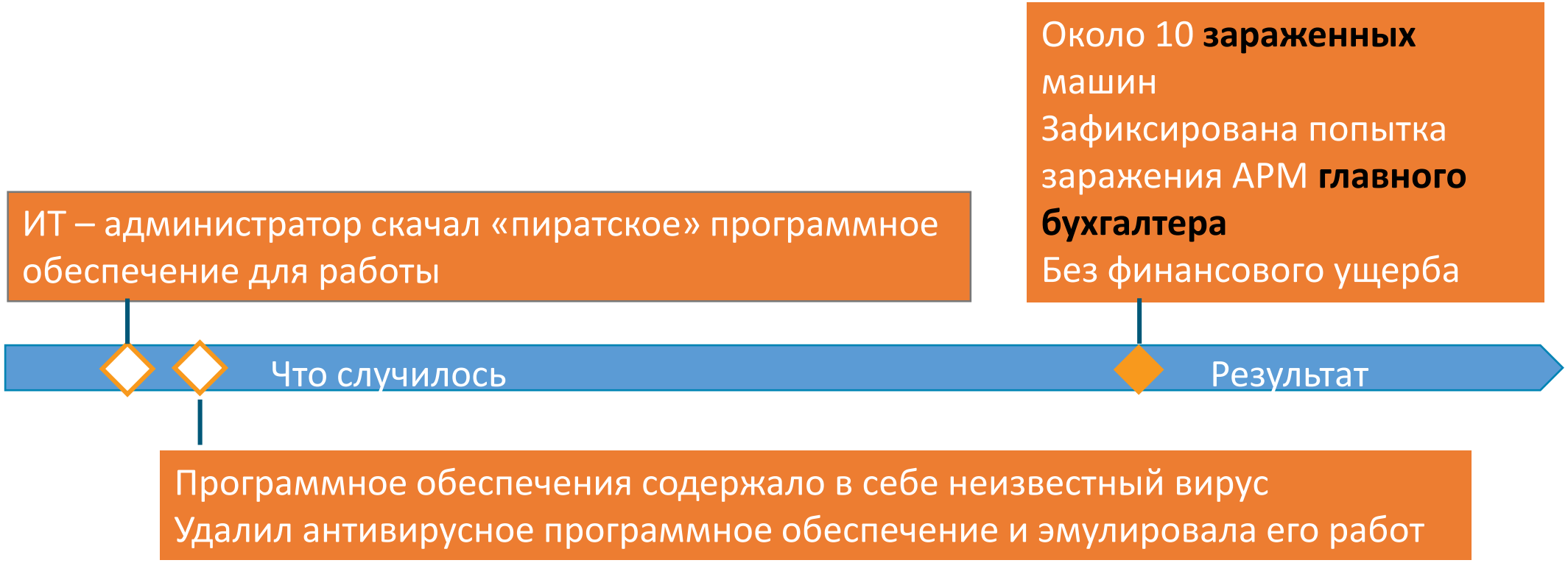
Кибербезопасность в МФЦ

Возможные векторы атак



Кибербезопасность в МФЦ

Пример реализации атаки



Кибербезопасность в МФЦ

Опыт создания систем кибербезопасности

1. Обследование и выявление защищаемой информации и ресурсов. Определение для них актуальных угроз и векторов атак.
2. Разработка технических и организационных решений по безопасности, включая типовые для разных уровней (муниципального, регионального, федерального).
3. Внедрение системы защиты информации и ее оценка соответствия (аттестация) требованиям по безопасности.
4. Организация непрерывного мониторинга защищенности объектов и реагирования на инциденты безопасности.

Опыт сотрудничества в регионах

Хабаровский край – сотрудничество по части организации мониторинга ИБ 24х7

Поволжский край – сотрудничество по части взаимодействие с ГосСОПКА и мониторинга инцидентов ИБ 24х7

Центральный регион – сотрудничество по части взаимодействия с ГосСОПКА, мониторинга инцидентов ИБ 24х7 и защиты веб-порталов

Крупнейшие региональные энергетические компании – обеспечение ИБ критичных сегментов на время проведения чемпионата мира

СПАСИБО!

КАСПИЙСК

11 октября, 2018