КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

29 ноября 2018
Калининград

#CODEIB

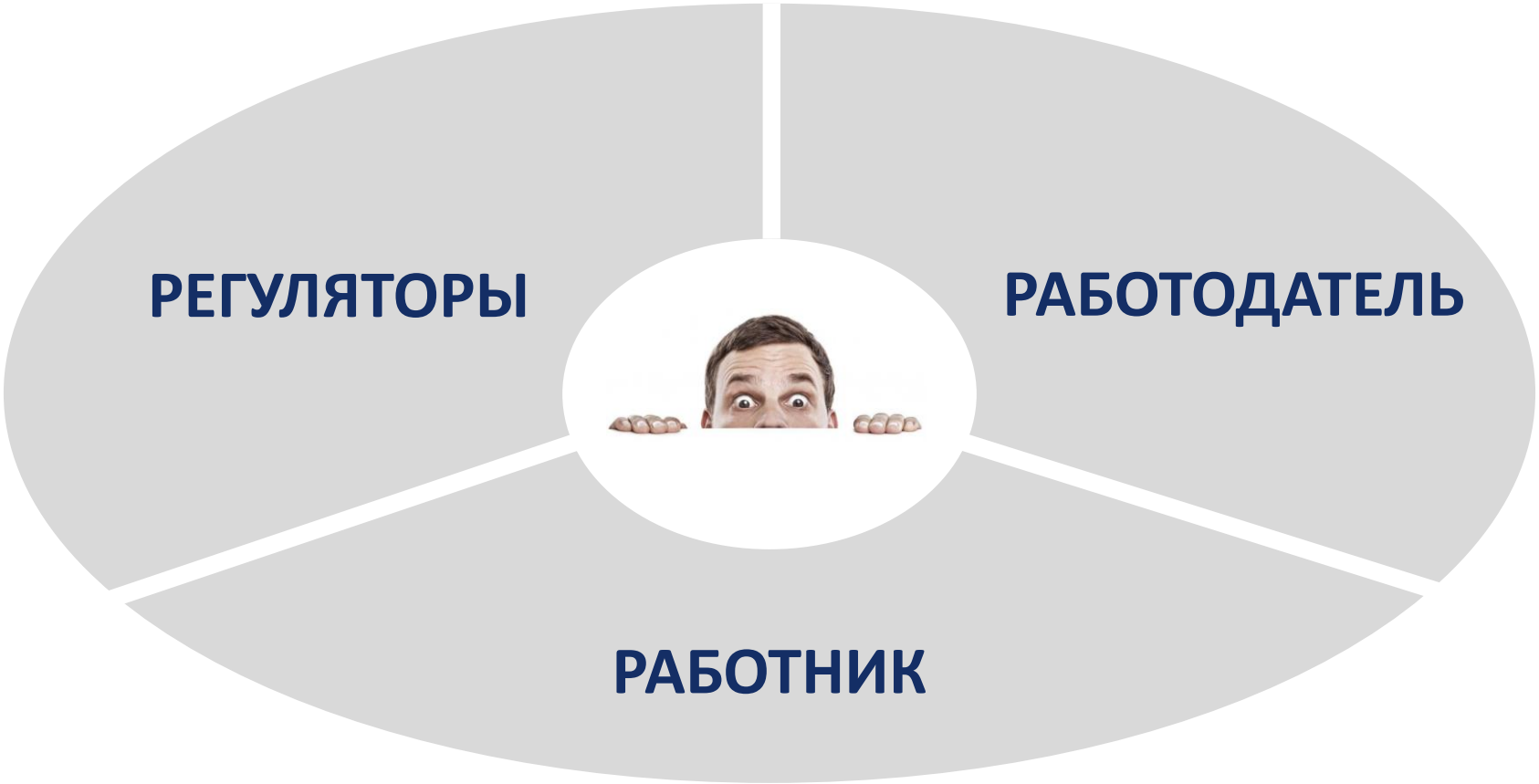
falcongaze

Менеджмент инцидентов информационной безопасности

Соколов Алексей

Руководитель отдела продаж г. Санкт-Петербург

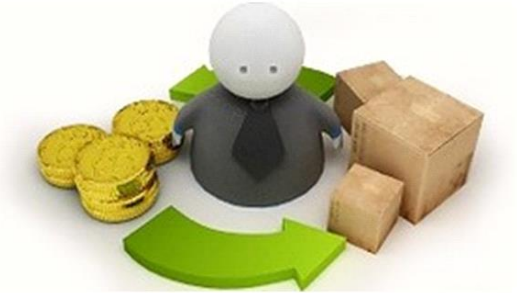
ВНЕДРЕНИЕ DLP. КАК УЧЕСТЬ ТРЕБОВАНИЯ, ПРАВА И ИНТЕРЕСЫ?



ИНВЕНТАРИЗАЦИЯ ИНФОРМАЦИОННЫХ АКТИВОВ ОРГАНИЗАЦИИ

Модель информационных активов организации

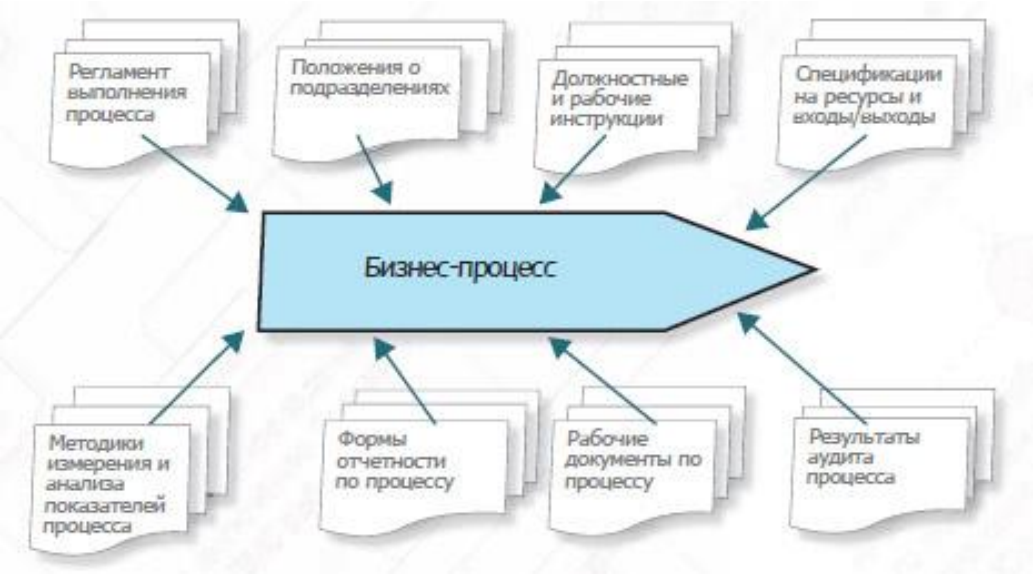
- **Информационные ресурсы**
  - ✓ Открытая (общедоступная) информация
  - ✓ Информация с ограниченным доступом
  - ✓ Информация охраняемая законами РФ
- **ИТ-инфраструктура**
  - ✓ Системы обработки и анализа информации (технические и программные средства её обработки, телекоммуникации, передачи и отображения)
  - ✓ Системы и средства защиты информации
  - ✓ Объекты и помещения с чувствительными компонентами АИС
- **Информационно-технологические процессы**
  - ✓ Процедуры сбора, обработки, хранения, передачи и уничтожения информации
- **Заинтересованные стороны**
  - ✓ Руководство организации
  - ✓ Персонал взаимодействующих организаций
  - ✓ Персонал конкурентных организаций



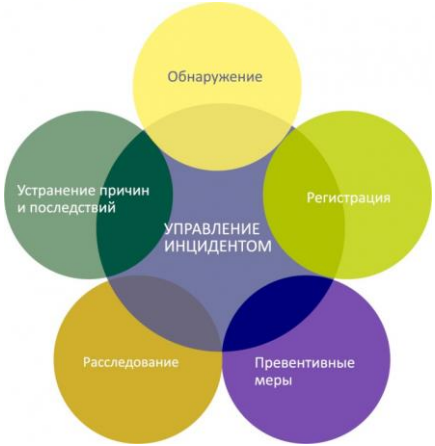
Актив – это всё что имеет ценность

ИНФОРМАЦИННЫЕ АКТИВЫ КАК СОСТАВЛЯЮЩАЯ БИЗНЕС-ПРОЦЕССОВ

- **Основные бизнес-процессы генерируют доходы предприятия;**
- **Информационные активы – одна из составляющих бизнес-процессов;**
- **Владелец бизнес-процесса – владелец связанных информационных активов.**



РАЗРАБОТКА ПОЛИТИК МЕННЕДЖМЕНТА ИНЦИДЕНТОВ ИБ



Менеджмент инцидентов ИБ
(ISO/IEC 27001:2013)

- Политика менеджмента событий ИБ
- Регламент реагирования на инцидент ИБ
- Регламент сбора доказательств
- Политика управления инцидентами ИБ

Оформление инцидента ИБ

1. Оформление Акта по инциденту ИБ.
2. Заключение экспертной комиссии компании.
3. Заключение комиссии по кадровым.
4. Выписка из системы учета рабочего времени.
5. Взятие объяснительной с сотрудника.
6. Заключение компьютерно-технической экспертизы по инциденту ИБ.

ПРИМЕЧАНИЕ: https://www.cbr.ru/credit/Gubzi_docs/stnd/

ПРИМЕРЫ ПРИЛОЖЕНИЙ РЕГЛАМЕНТОВ

1. Перечень информации ограниченного доступа (ПДн, КТ, СТ, БТ, ВТ. и пр.).
2. Запрет разглашения информации ограниченного доступа.
3. Положения об ответственности работников.
4. Положение по информации ограниченного доступа.
5. Положение о коммерческой тайне
6. Правила обработки и защиты информации.
7. Запрет хранения личной информации на корпоративных устройствах.
8. Положение о конфиденциальной информации (Положение о конфиденциальности).
9. Типовой раздел по конфиденциальности в трудовом или гражданско-правовом договоре (дополнительном соглашении к договору).
10. Памятка работнику о сохранении коммерческой тайны.
11. Типовые правила использования средств хранения, обработки и передачи информации.
12. Типовой регламент контроля использования технических средств хранения, обработки и передачи информации работниками Организации.
13. Политика управления инцидентами информационной безопасности.
14. Парольная политика.
15. Положение о сборе доказательств за периметром организации.
16. Регламент использования корпоративной электронной почты.

РАБОТА С ИНЦИДЕНТАМИ

- **Этап Планирование и подготовка**
- Политика менеджмента ИБ
- Программа менеджмента ИБ
- Политики менеджмента рисков и ИБ
- Создание группы реагирования на инциденты ИБ
- Техническая и другая поддержка реагирования на инциденты ИБ
- Обеспечение осведомлённости и обучение
- **Этап Использование**
- Ключевые процессы
- Обнаружение и оповещение о событиях информационной безопасности
- Оценка и принятие решений по событиям/инцидентам
- Реагирование на инциденты
- **Этап Анализ**
- Правовая экспертиза
- Извлечённые уроки
- Определение улучшений безопасности
- Определение улучшений системы
- **Этап Улучшение**
- Улучшение анализа рисков и менеджмента безопасности
- Осуществление улучшений безопасности.
- Осуществление улучшений системы.
- Другие улучшения.

СТАТИСТИКА СУДЕБНЫХ РЕШЕНИЯМ ПО «DLP-СТАТЬЯМ» В 2017 г.

	Статья УК РФ	Число осуждённых
183 ч. 1	Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну	0
183 ч. 2	Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну	5
183 ч. 3	Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну При отягчающих обстоятельствах	8
185.6 ч. 1	Умышленное использование инсайдерской информации для осуществления операций с финансовыми инструментами	0
185.6 ч. 2	Умышленное использование инсайдерской информации путём её неправомерной передачи другому лицу	0

Источник: http://80na20.blogspot.com/2018/04/blog-post_11.html

ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Зарубежные стандарты сертификации кибер-юристов

- **CCCI (Certified Computer Crime Investigator)**
  Сертифицированный следователь по компьютерным преступлениям

- **CCFT (Certified Computer Forensic Technician)**
  Сертифицированный компьютерный судебный техник

- **CCCP (Certified Computer Crime Prosecutor)**
  Сертифицированный прокурор по компьютерным преступлениям

- **CCCA (Certified Computer Crime Attorney)**
  Сертифицированный адвокат по компьютерным преступлениям

Отечественный образовательный стандарт

?

40.04.01 «Юриспруденция»
ИНФОРМАЦИОННОЕ ПРАВО

2017г. «Цифровая экономика Российской Федерации»

2.4.4. С учетом требований к компетенциям цифровой экономики обновлены образовательные программы всех уровней образования в целях использования в учебной деятельности, в том числе при государственной итоговой аттестации, общепользовательских и профессиональных цифровых инструментов
IV квартал 2020 г.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

29 ноября 2018
Калининград

#CODEIB

falcongaze

Спасибо за внимание!

Соколов Алексей

Руководитель отдела продаж г. Санкт-Петербург

+7 (951) 681-38-40
a.sokolov@falcongaze.ru