КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13 июня 2019
Калининград

#CODEIB

falcongaze

Менеджмент инцидентов информационной безопасности

Соколов Алексей

Руководитель отдела продаж г. Санкт-Петербург

ВНЕДРЕНИЕ DLP. КАК УЧЕСТЬ ТРЕБОВАНИЯ, ПРАВА И ИНТЕРЕСЫ?

РЕГУЛЯТОРЫ

РАБОТОДАТЕЛЬ

РАБОТНИК

Информационные ресурсы

Открытая (общедоступная) информация

Информация с ограниченным доступом

Информация охраняемая законами РФ

ИНВЕНТАРИЗАЦИЯ ИНФОРМАЦИОННЫХ АКТИВОВ ОРГАНИЗАЦИИ

ИТ-инфраструктура

ИТ-процессы

- ✓ Сбор
- ✓ Обработка
- ✓ Хранение
- ✓ Передача
- ✓ Уничтожение

информации

Заинтересованные стороны

Персонал взаимодействующих организаций

Персонал конкурентных организаций

Руководство организации

ИНФОРМАЦИОННЫЕ АКТИВЫ В БИЗНЕС-ПРОЦЕССАХ

Бизнес-процессы генерируют доходы предприятия

Информационные активы – важная составляющая бизнес-процессов

Владелец бизнес-процесса – владелец связанных информационных активов

ИНФОРМАЦИОННЫЕ АКТИВЫ В БИЗНЕС-ПРОЦЕССАХ

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

falcongaze™

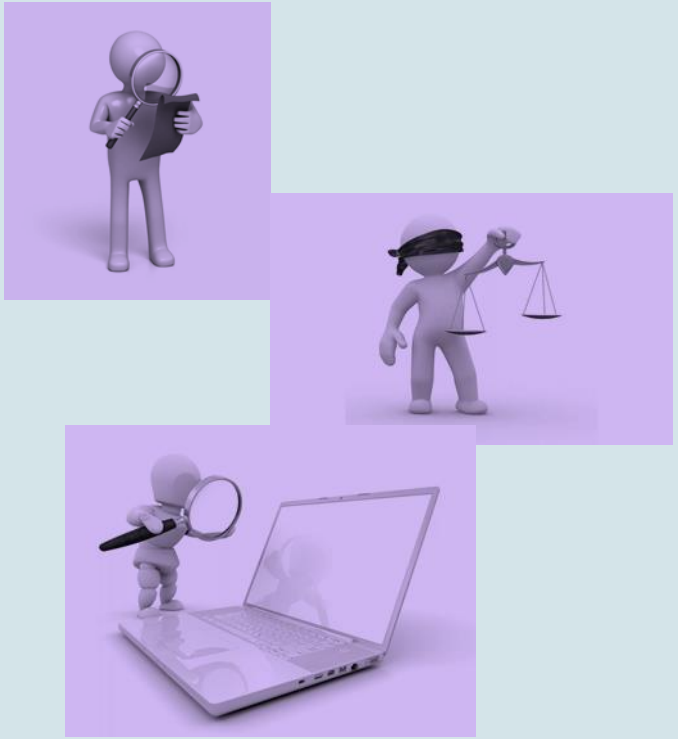
ПРИМЕРЫ ПРИЛОЖЕНИЙ РЕГЛАМЕНТОВ МЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИБ

- Правила обработки и защиты информации
- Перечень информации ограниченного доступа
- Положения об ответственности работников
- Парольная политика
- Положение о коммерческой тайне
- Политика управления инцидентами информационной безопасности

ГРУППА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ГРИИБ)

- Information Security Incident Response Team (ISIRT): Группа обученных и доверенных членов организации

- Данная группа обрабатывает инциденты ИБ во время их жизненного цикла и иногда может дополняться внешними экспертами.



falcongaze™

ДОКУМЕНТАРНОЕ ОФОРМЛЕНИЕ ИНЦИДЕНТОВ

- Оформление Акта по инциденту ИБ
- Заключение экспертной комиссии компании
- Заключение комиссии по кадровым вопросам
- Выписка из системы учета рабочего времени
- Взятие объяснительной с сотрудника
- Компьютерно-техническая экспертиза по инциденту ИБ

ЭТАПЫ РАБОТЫ С ИНЦИДЕНТАМИ ИБ

Планирование и подготовка

Анализ

Использование

Улучшение

falcongaze™

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

5
человек
ст. 183 ч. 2

8
человек
ст. 183 ч. 2

Осуждены за незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну

Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну
При отягчающих обстоятельствах

falcongaze™

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

А как у нас?

40.04.01 «Юриспруденция»
ИНФОРМАЦИОННОЕ ПРАВО

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13 июня 2019
Калининград

#CODEIB

falcongaze

Спасибо за внимание!

Соколов Алексей

Руководитель отдела продаж г. Санкт-Петербург

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