КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | КРАСНОЯРСК

23.03.2023

ОБОМНЕ

- **Туговиков Виктор Борисович,**
- **Сибирский федеральный университет,**

  Институт космических и информационных технологий,

  Кафедра информационной безопасности,

  доцент, к.ф.м-н.

  Эксперт в области систем управления информационной безопасностью.

  VTugovikov@sfu-kras.ru

Восемь навыков CISO (или, как создать идеальную команду ИБ)

Особенности национальной ИБ:

Подчинённость СБ

Подчинённость ИТ

Мировая практика:

Подчинённость CEO

Подчинённость HR

Уровни соответствия ИБ требованиям ГОСТ и законодательству РФ (Уровень зрелости):

0: финансирование отсутствует, ИБ никто не занимается;

1: финансирование ведется в рамках общего бюджета ИТ, ИБ рассматривается как чисто техническая проблема ИТ;

2: финансирование ведется в рамках отдельного бюджета, ИБ рассматривается руководством как комплекс организационных и технических мероприятий;

3: финансирование ведется в рамках отдельного бюджета, ИБ вертикально интегрирована, является частью корпоративной культуры, назначен CISO.

Должности и навыки в ИБ (таблица из Интернет)

	CISO	Архитектор ИБ	Консультант ИБ	Аналитик ИБ	Специалист по обучению	Менеджер по операциям ИБ	Менеджер по непрерывности бизнеса	Специалист по физической безопасности
Визионер	☑							
Командир	☑	☑				☑	☑	
Писатель	☑		☑	☑	☑		☑	
Презентатор	☑	☑	☑	☑	☑		☑	
Архитектор								☑
Консультант		☑	☑	☑			☑	
Технический гуру		☑	☑					
Учитель		☑	☑		☑			
Искатель талантов	☑							
Продавец	☑	☑	☑		☑		☑	
Планировщик	☑				☑		☑	☑
Переговорщик	☑	☑	☑			☑		
Исполнитель			☑		☑	☑	☑	☑
Исследователь				☑				
Аудитор						☑		☑
Техник						☑	☑	☑

	CISO	Архитектор ИБ	Консультант ИБ	Аналитик ИБ	Специалист по обучению	Менеджер по операциям ИБ	Менеджер по непрерывности бизнеса	Специалист по физической безопасности
Визионер	☑							
Командир	☑							
Писатель	☑							
Презентатор	☑							
Архитектор								
Консультант								
Технический гуру								
Учитель								
Искатель талантов	☑							
Продавец	☑							
Планировщик	☑							
Переговорщик	☑							
Исполнитель								
Исследователь								
Аудитор								
Техник								

Основные навыки зама по информационной безопасности:

1. Знать все нюансы и особенности бизнес-процессов организации.
2. Предвидеть возникновение угроз ИБ в контексте развития информационных технологий, автоматизации, цифровизации бизнес-процессов.
3. Быстро принимать решения как локального, так и стратегического характера.
4. Грамотно вести служебную переписку, кратко и убедительно писать обоснования по мерам ИБ.
5. Уметь делать убедительные презентации проектов ИБ.
6. Талант убеждения (грамотная устная речь, коммуникабельность, доброжелательность, вежливость, эмоциональная устойчивость)
7. Грамотно подбирать персонал ИБ, с учётом навыков и склонностей.
8. Умение работать в команде и выстраивать команду ИБ.

Идеальная команда ИБ – когда весь персонал, каждый на своём месте, ответственно относится к ИБ.

Немного теории

S = f(F,A,L,C, P) - полная безопасность системы,

В данной формуле:
F - физическая безопасность,
A - администрирование,
L - безопасность при передаче данных,
C - безопасность компьютерной обработки данных,
P - персональная безопасность (ответственность, лояльность и сознательность).

Каждый элемент может изменяться в интервале от 0 до 1.
Очень хорошая защита находится в интервале от 0,8 до 0,9, значение, меньшее, чем 0,3 говорит о неудовлетворительном уровне безопасности информации.

Немного теории

Допустим у нас есть K работников, которые имеют доступ к N информационных объектов:

P_M= Min { p_1, … ,p_K} – параметр безопасности M-го объекта доступа характеризующий уровень защищенности информации, зависящий от человеческого фактора.

В данной формуле:
p_i - уровень благонадежности i-й персоной,
значения p_i определены на отрезке [0,1), то есть уровень благонадёжности может изменяться в интервале от 0 – что означает полную невыполнимость сохранения конфиденциальности, до 1 - полная благонадежность, что в принципе не достижимо.
i=1,…K

Из формулы следует, что если у одного, скажем, p_i-того сотрудника, значение уровня благонадёжности опускается ниже критического значения 0.3, то значение параметра P_M безопасности объекта тоже становится ниже 0.3 (высокий уровень угрозы информации M-го объекта).

Немного теории

В формуле $P_M = Min \{ p_1, \dots, p_K \}$ значения уровня благонадежности каждого работника не постоянны во времени:

$$p_i = p_i (\Theta_+, \Theta_-, t)$$

В данной формуле:
t – время;

$\Theta_+ (t)$ - параметр определяемый совокупностью усиливающих персональную ответственность внешних воздействий (*доплаты, поощрения, наличие контроля, боязнь потерять работу, амбиции к карьерному росту*** …);**

$\Theta_- (t)$ - параметр определяемый совокупностью понижающих персональную ответственность внешних воздействий (*плохое отношение руководства, тяжелые жизненные ситуации, возможности перехода на более перспективную работу к конкурентам***…).**

Методика оценки угроз безопасности информации ФСТЭК .

Основные виды нарушителей:

Подсказки из практики

- ✓специальные службы иностранных государств;
- ✓террористические, экстремистские группировки;
- ✓преступные группы (криминальные структуры);
- ✓отдельные физические лица (хакеры);
- ✓конкурирующие организации;
- ✓разработчики программных, программно-аппаратных средств;
- ✓лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- ✓поставщики услуг связи, вычислительных услуг;
- ✓лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- ✓лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем организации (администрация, охрана, уборщики и др.);
- ✓авторизованные пользователи систем и сетей;
- ✓системные администраторы и администраторы безопасности;
- ✓бывшие (уволенные) работники - пользователи систем.

Как привлечь персонал к вопросам обеспечения ИБ :

Подсказки из практики

1. **Повышение IT – грамотности.**
2. **Повышение ИБ – грамотности.**
3. **Возложение ответственности за выполнение мер ИБ на пользователей.**
4. **Возложение ответственности за ИБ на руководителей.**
5. **Контроль выполнения мер ИБ.**

КИБЕРДРУЖИНА

Как привлечь персонал к вопросам обеспечения ИБ?

Подсказки из практики

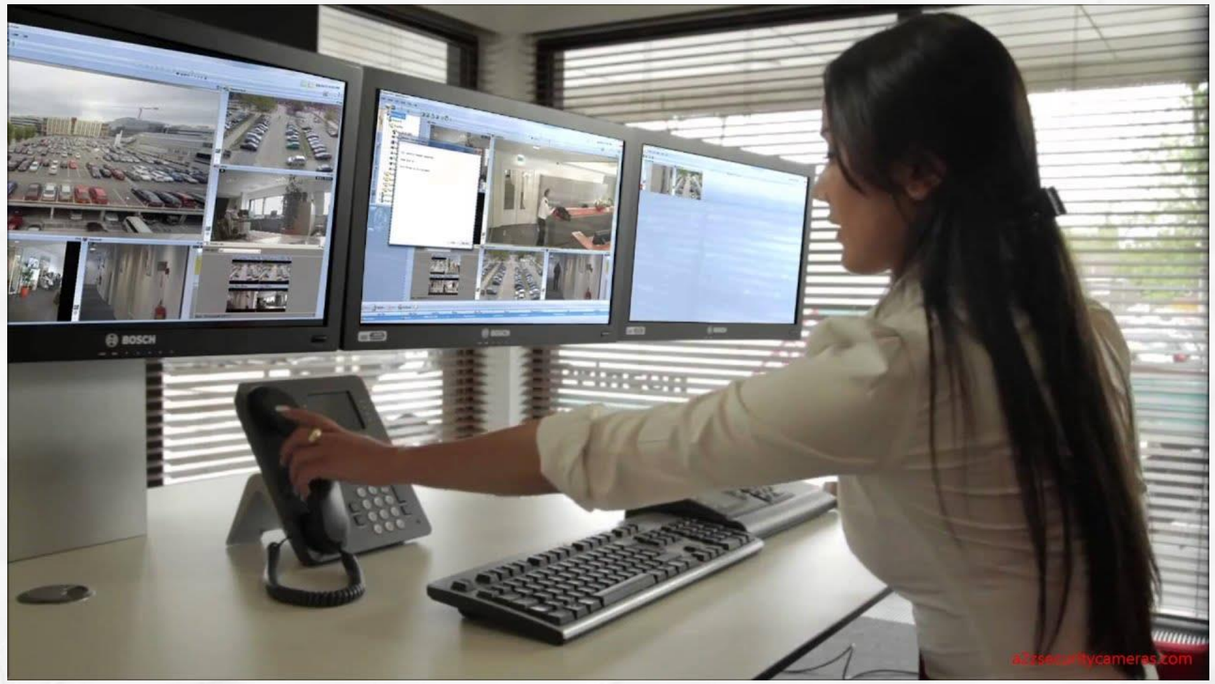
Как выстроить ИБ как вертикально интегрированный процесс?

КИБЕРДРУЖИНА

Контроль выполнения мер ИБ:

Взаимодействие ИБ с IT:

Для сетевых администраторов, администраторов систем, нужны отдельные инструкции, ориентированные на правила выполнения ИБ привилегированными пользователями.



Готов ответить
на ваши вопросы

Туговиков Виктор Борисович
E-mail: VTugovikov@sfu-kras.ru

По вопросам курсов повышения квалификации и курсов переподготовки обращаться по адресу:
OGrigoreva@sfu-kras.ru (Ольга Валерьевна)