deiteriy compliance

Внедрение 716-П. Изменение привычной работы отдела ИБ

АЛЕКСАНДР ИВАНЦОВ | Deiteriy | Конференция АБИСС, Москва 2022

Александр Иванцов

Старший инженер по защите информации

Deiteriy

aleksandr.ivantsov@deiteriy.com

т. +7 (812) 361-61-55

м. +7 (911) 785-97-96

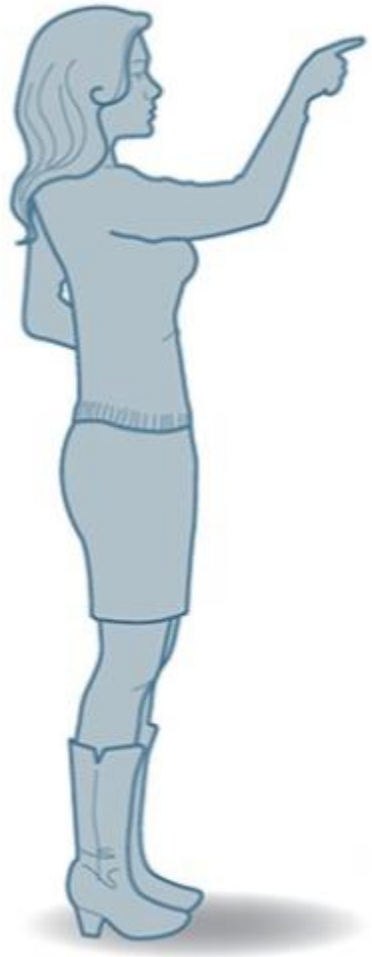
Актуальность темы

1. 716-П связал риски информационной безопасности и операционные риски.

2. У отделов ИБ и управления рисками свои взгляды на саму природу риска и отношение к нему.

3. 716-П рассматривает риски ИБ как операционные риски и ставит задачу прийти к единому пониманию риска ИБ.

Разница в терминологии



Событие операционного риска информационной безопасности	Инцидент информационной безопасности
База событий операционного риска	Журнал инцидентов
Самооценка операционных рисков	Оценка рисков информационной безопасности
Ключевые индикаторы риска	События и параметры мониторинга

Кто же должен заниматься рисками ИБ как частью операционных рисков?

Риски информационной безопасности входят в операционные риски и обладают всеми элементами классификации и параметрами, присущими операционным рискам.

Даже в самом Положении № 716-П учитывается особая природа рисков информационной безопасности и их отличие от остальных операционных рисков, определены отдельные критерии, применимые только к рискам информационной безопасности.

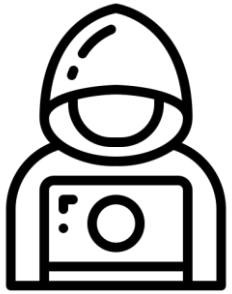
Кто же должен заниматься рисками ИБ как частью операционных рисков?

Вывод: невозможно охватить всю тему работы с рисками информационной безопасности как с операционными рисками силами одного отдела.

Новые вопросы:

1. Проведение границы обязанностей и ответственности между подразделениями
2. Построение системы взаимодействия

Совместная работа

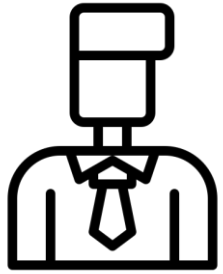


Выявление инцидентов
Сбор информации
Регистрация инцидента
Оценка потерь

Оценка рисков ИБ

Регистрация события операционного риска
Фиксирование количественных и качественных потерь

Самооценка операционного риска



3 изменения в работе отдела ИБ

1

Обработка инцидентов – «событий риска информационной безопасности»

2

Определение метрик эффективности системы управления рисками ИБ, контроль показателей

3

Оценка рисков информационной безопасности

Обработка инцидентов

Процедуры мониторинга и реагирования остаются без изменений

Изменяется:

1. Оценка финансовых потерь и сравнение с пороговым значением (относится ли к событиям риска ИБ)
2. Классификация и формат регистрации
3. Подсчет потерь
4. Регистрация «отраженных» инцидентов

Метрики эффективности системы управления рисками ИБ

Контрольные показатели уровня операционного риска – глобальные показатели, установленные для организации (процесса) в целом. Используются в целях контроля процесса управления операционными рисками и выявление глобальных проблем.

Ключевые индикаторы риска (КИР) – индикаторы, установленные для каждого риска в отдельности. Используются в целях обнаружения факта реализации риска.

Метрики эффективности системы управления рисками ИБ

КИР	КПУОР
Устанавливаются для каждого риска	Устанавливаются в общем, глобально
Могут считаться средствами автоматизации	Считаются на основе статистики событий ОР за последние 10 лет
Нужно придумать пороговые значения	Нужно придумать сигнальные и контрольные пороговые значения, но есть ограничения в 716-П
Нужно придумать порядок реагирования на превышение порога	Порядок реагирования: Превышение сигнального значения – ежедневный мониторинг Превышение контрольного значения – сообщение совету директоров + дополнительные придуманные и задокументированные меры
Устанавливается периодичность мониторинга, производится расчет	Устанавливается периодичность мониторинга, производится расчет
Ежегодный пересмотр	Ежегодный пересмотр

Оценка рисков ИБ

Общий процесс – самооценка операционного риска.

Подразделение ИБ проводит оценку рисков ИБ и передает результаты подразделению по управлению рисками в целях их добавления к самооценке по всем операционным рискам.

Изменения относительно «классического» процесса оценки рисков ИБ:

1. Классификация
2. Формат результата

Спасибо за внимание!

Александр Иванцов

Старший инженер по защите информации

Deiteriy

aleksandr.ivantsov@deiteriy.com

т. +7 (812) 361-61-55

м. +7 (911) 785-97-96