

Теория информационной безопасности и методология

Лекция 3

к.т.н., доцент ФБИТ
Коржук Виктория Михайловна

2023

Предыдущая лекция

1. Примеры разрушительных кибер-атак
2. Задача оценки угроз ИБ
3. Система показателей уязвимости
4. Подходы к оценке уязвимости
5. Рекомендации по предъявлению требований к ЗИ
6. Определение основного требования ЗИ
7. Информация как ресурс и как объект труда
8. Показатели (свойства информации)

Триады ИБ

конфиденциальность

целостность

доступность

уязвимость

дестабилизирующий фактор

угроза

событие ИБ

атака

инцидент ИБ



Событие vs инцидент

В чем разница между событием и инцидентом ИБ?

Collaborate!

Событие vs инцидент

Событие vs инцидент

- установленное возникновение состояния системы, службы или сети, указывающее на возможное нарушение политики информационной безопасности или сбой в работе средств управления, или на ранее неизвестную ситуацию, которая может иметь отношение к безопасности.

- одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают информационной безопасности.



Что такое дестабилизирующий фактор?

Collaborate!


Что такое дестабилизирующий фактор?

Дестабилизирующие факторы

- такие явления или события, которые могут появляться на каком-либо этапе жизнедеятельности информационной системы и следствием которых могут быть нежелательные (в смысле защищенности) воздействия на информацию.

1. количественная недостаточность элементов информационной системы;
2. качественная недостаточность составляющих систему элементов;
3. отказы элементов;
4. сбои и ошибки элементов;
5. стихийные бедствия;
6. злоумышленные действия;
7. побочные явления.

Соедините между собой виды дестабилизирующих факторов и их определения.

			своих функций
отказ	 временное нарушение работоспособности конструкции вследствие чего функции выполняются		несовершенство конструкции или неэффективная организация взаимодействия одного или нескольких элементов ИС

Matching Pairs

Функция защиты информации

- совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в ИС различными средствами и методами с целью создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Требование полноты множества функций: при надлежащем обеспечении соответствующего уровня осуществления каждой из функций множества гарантировано может быть достигнут требуемый уровень защищенности информации.

Непрерывный и
V

функции непосредственной
защиты информации

управляемый
процесс
V

механизмы управления
функциями непосредственной
защиты информации

Задачи защиты информации

- возможности средств, методов и мероприятий, реализуемых в ИС с целью осуществления функций защиты.

1. Требуемый уровень защиты при минимальных затратах

2. При заданных затратах - максимальный уровень защиты.

В чем вопрос?

Требования к ЗИ -
установлены,

а методы ЗИ -
относительны.

Какими могут быть итоговые события?



Подумайте, какие 3 исхода могут произойти в результате процесса защиты информации?

Collaborate!

Какими могут быть итоговые события?

Итоговые события

Событие №1 - защита информации обеспечена, поскольку даже при условии проявления дестабилизирующих факторов предотвращено их воздействие на защищаемую информацию или ликвидированы последствия такого воздействия.

Событие №2 - защита информации нарушена, поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано.

Событие №3 - защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано.



Множество функций защиты

Функция №1 - предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов.

Функция №2 - предупреждение непосредственного проявления дестабилизирующих факторов в конкретных условиях функционирования ИС.

Функция №3 - обнаружение проявившихся дестабилизирующих факторов.

Функция №4 - предупреждение воздействия дестабилизирующих факторов на защищаемую информацию: обнаруженных (4а) и не обнаруженных (4б).

Функция №5 - обнаружение воздействия дестабилизирующих факторов на защищаемую информацию.

Функция №6 - локализация воздействия дестабилизирующих факторов на информацию: обнаруженного воздействия (6а) и не обнаруженного воздействия (6б).

Функция № 7 - ликвидация последствий воздействия дестабилизирующих факторов на защищаемую информацию: обнаруженного и локализованного (7а) и локализованного, но

Приведите п  функции 3

Приведите пример функции с обнаружение проявившихся
дестабилизирующих факторов.

Collaborate!

Приведите пример функции 3

Приведите пример функции 4 – предупреждение
воздействия



Функция 4а – проявившихся и обнаруженных ДФ, 4б – проявившихся и

Collaborate!

Приведите пример функции 4 - предупреждение воздействия

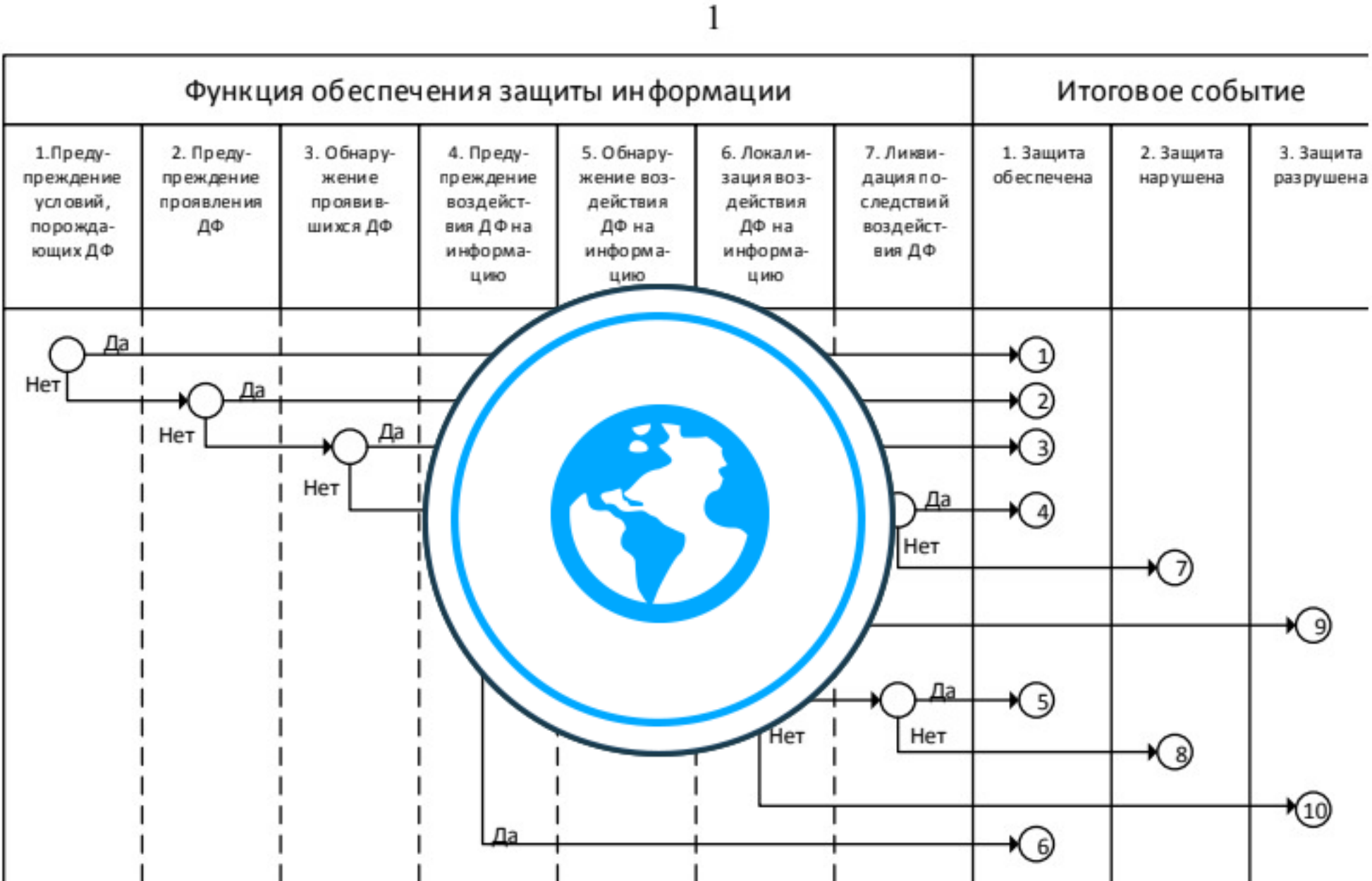
Приведите примеры функции 6 – локализация

6а – обнаруженного воздействия, 6б – необнаруженного воздействия

Collaborate!

Приведите примеры функции 6 - локализация

Про вероятности



<https://drive.google.com/file/d/1fPuVdIfQfxNhYX8AkuSN6-ojY0EKbVww/view?usp=sharing>

Рисунок 1. Общая модель исходов при осуществлении функции обеспечения защиты информации (ДФ дестабилизирующих фактор)

Каждый из исходов является событием случайным, а все они вместе составляет полную группу несовместных событий. Как известно из теории



Четыре функции управления

4,343 views • Dec 18, 2017



394



2



SHARE



SAVE



Andrev K

Up next



You're signed out of YouTube

Sign in to like videos, comment, and subscribe.

GOT IT



Классическая теория управления (1900-1930):...

Andrey K

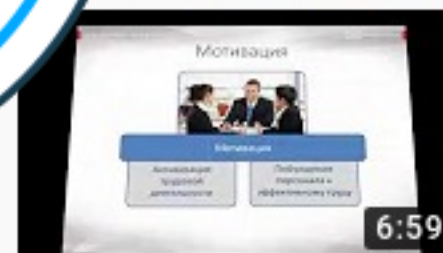
14K views • 2 years ago



Менеджмент простыми словами

GarageBiz

60K views • 1 year ago



05 Функции менеджмента

Университет СИНЕРГИЯ

38K views • 7 years ago



МАГНЕТАР, САМЫЙ ОПАСНЫЙ МАГНИТ ВО...

<https://www.youtube.com/watch?v=yd1Kxa1zjkw>

организации, должен мыслить стратегически и концептуально для того чтобы достигать целей организации. На этом уроке будут описаны

SHOW MORE

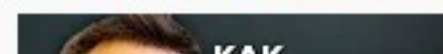


Навальный об обнулении Путина

Новости СМЕХдержарвы

Recommended for you

New



Как Планирует День ИЛОН

Quiz

Пожар относится к...

- ☐ событиям ИБ
- ☐ инцидентам ИБ
- ☐ дестабилизирующим факторам

Какие выражения имеют место быть?

- Нужно обеспечить максимальный уровень защищенности при заданных затратах.
- Нужно максимизировать требования ко всем функциям защиты для обеспечения требуемого уровня защищенности
- Нужно минимизировать затраты, добившись заданного уровня защищенности.

Сколько исходов приводит к нарушению защиты?

- ☐ 6
- ☐ 2
- ☐ 10

Сколько исходов приводит к разрушению защиты?

☐ 6

☐ 2

☐ 1

Совокупность мероприятий, осуществляемых в ИС различными средствами и методами с целью создания, поддержания и обеспечения условий, необходимых для надежной защиты информации - это...

- ☐ задача защиты информации
- ☐ функция защиты информации
- ☐ событие ИБ
- ☐ исход при реализации функции защиты
- ☐ полное множество защиты



Exit ticket

Что вы сегодня узнали? Какие остались вопросы? Какие есть комментарии?

Collaborate!

Exit ticket