

Теория информационной безопасности и методология

Лекция 4 Функции защиты информации

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

весна, 2023

Предыдущая лекция



1. ДФ, событие, инцидент
2. Задачи ЗИ
3. Итоговые события нарушения ИБ
4. Функции ЗИ
5. Функции управления ИБ

Надежная система ИБ

Абсолютно безопасных систем
нет.

Политика ИБ

+

Есть такие, которым можно
доверять.

Гарантированность



Итоговые события ИБ

Collaborate!

Итоговые события ИБ

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

Сведение репрезентативного множества задач защиты в классы

Множество задач защиты $Z = F * Z * V * D$, где

F - множество функций защиты;

Z - множество зон защиты;

V - множество видов защиты;

D - множество дестабилизирующих факторов, влияющих на защищенность информации.

Расчет множества задач защиты



По формуле $Z^* = \Phi \times Z \times V \times D$ посчитайте размер множества задач защиты и объясните выбранные показатели

Collaborate!

Расчет множества задач защиты

Классификация задач защиты

№ функции	Функция	Пути реализации на этапах жизненного цикла ИС		
		Создание	Внедрение	Эксплуатация
1	Предупреждение проявления условий, благоприятных для порождения дестабилизирующих факторов	1.Обоснование требований к защите информации по всей совокупности показателей 2.Формирование множества дестабилизирующих факторов 3.Оценка возможных последствий воздействия факторов 4.Проектирование к устойчивых к факторам	1.Проверка и уточнение требований к защите информации 2.Проверка и уточнение требований к устойчивости к дестабилизирующим факторам 3.Проверка проектных решений	1.Обеспечение работы механизмов предупреждения 2.Контроль работы механизмов предупреждения 3.Сбор и обработка статических данных о работе механизмов предупреждения 4.Разработка предложений по совершенствованию механизмов предупреждения
2	Предупреждение проявления дестабилизирующих факторов	1.Обоснование требований к слежению за функционированием компонентов предупреждения появления условий, предусмотренных функцией №1 2.Проектирование механизмов слежения	1.Проверка и уточнение требований к механизмам слежения 2.Проверка проектных решений по вопросам слежения	1.Обеспечение работы механизмов слежения 2.Контроль работы механизмов слежения 3.Сбор и обработка данных о
		благоприятных для дестабилизирующих факторов		4.Разработка предложений по совершенствованию механизмов слежения

<https://cf.nearpod.com/neareducation/new/Webpage/434019113/iconoriginal.pdf?AWSAccessKeyId=AKIA5LQSO4AXIHKV2NEC&Expires=2147483647&Signature=wSFfCDtkVbayzmGb1BOfC0hh1KM%3D>

Классы задач ЗИ

1. введение избыточности элементов системы
2. резервирование элементов системы
3. регулирование доступа к элементам системы
4. регулирование использования элементов системы
5. маскировка информации
6. контроль элементов системы
7. регистрация сведений
8. уничтожение информации
9. сигнализация
10. реагирование

Приведите пример  ния избыточности
системы

Collaborate!

Приведите пример введения избыточности системы



Приведите пример резервирования элементов системы

Collaborate!

Приведите пример резервирования элементов системы

Приведите пример регулирования доступа к
элементам системы



Collaborate!

Приведите пример регулирования доступа к элементам системы

Пример регулирования использования
элементов системы



Collaborate!

Пример регулирования использования элементов системы



Приведите пример маскировки информации

Collaborate!


Приведите пример маскировки информации



Приведите пример контроля элементов системы

Collaborate!

Приведите пример контроля элементов системы

Приведите пример  регистрации сведений

Collaborate!

Приведите пример регистрации сведений



Приведите пример уничтожения информации

Collaborate!

Приведите пример уничтожения информации



Приведите пример сигнализации в системе 3И

Collaborate!

Приведите пример сигнализации в системе 3И

Приведите пример реагирования системы
защиты информации



Collaborate!

Приведите пример реагирования системы защиты информации



1 2 3 4 5 6



Headings you add to the document will appear here.

You are suggesting

ЛР 4 Деловая игра по ИБ

Групп



любое крупное свершившееся событие в
собой большой ущерб (в финансовом,
плане). Цель игры - минимизировать ущерб,
ния.

сценарий события из 5 этапов: начальный, 3
промежуточные, заключительный. Для каждого этапа описать ситуацию
и составить набор "правильных" решений с учетом ролей (об этом ниже) с
точки зрения разработчиков игры. Обратите внимание, что несмотря на
выполнение действий на каждом этапе ситуация продолжает развиваться

https://docs.google.com/document/d/1YVdnAldDER4waJyDk3sxPhTjwOeaVQwgf_e3-K_eyrw/edit?usp=sharing

утонул, но всех спасли / Титаник успели отбуксировать на большую землю
и все спаслись)

3. Роли (3-6) необходимы для корректного выполнения решений





Вопросы/комментарии

Collaborate!

Вопросы/комментарии