*Утверждены на заседании кафедры компьютерной безопасности МИЭМ НИУ ВШЭ, протокол №5 от 24.06.2019*

Федеральное государственное автономное образовательное

учреждение высшего образования
Национальный исследовательский университет
«Высшая школа экономики»

Московский институт электроники и математики им. А.Н. Тихонова

Кафедра компьютерная безопасности

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

к выполнению курсовой работы

по дисциплине «Основы информационной безопасности»

МОСКВА 2019

**Цель работы**: научиться строить модель угроз и нарушителя согласно Методике определения угроз безопасности информации в информационных системах, разработанной Федеральной службой по техническому и экспортному контролю в 2015 г.

**Формат работы**: текстовый отчет со схемами и таблицами.

**Порядок работы:**

1. Выбрать объект информатизации и его компоненты.

Объектом может быть любая реально существующая или вымышленная организация (например, отделение полиции или библиотека). В рамках данной курсовой работы объект не может быть территориально-распределенным.

Компоненты – это определенные источники приема или отправления информации. Например, сервер или сотрудник приемной.

Объект и компоненты необходимо представить в виде схемы.

Количество компонентов определяется исходя из требований к количеству потоков информации, которые на схеме можно обозначить условно стрелками. Количество потоков информации (минимум): 3 потока внутренних (отправитель и получатель в границах объекта), 3 – изнутри объекта, 3 – внутрь объекта.

Показать границы объекта.

В границы объекта попадают компоненты, подчиняющиеся административным мерам защиты информации, принимаемым руководством организации. Взаимодействующие с объектом организации и лица располагаются вне его границ.

*Пример:*

**

1. Указать способы передачи данных для всех потоков информации.

Это можно сделать условными обозначениями над потоками информации на самой схеме, пояснения которых можно указать в приложении к работе.

*Пример:*

**

|  |  |
| --- | --- |
| *Условное обозначение* | *Описание* |
|  | *Бумажный носитель* |
|  | *Электронный файл* |
| *…* | *…* |

1. Указать свойства информации, которые необходимо обеспечить.

Над стрелками, обозначающими потоки информации, можно указать К, Ц, Д соответственно для конфиденциальности, целостности, доступности.

Обратите внимание, что указывать нужно те свойства, которые может обеспечить со своей стороны именно рассматриваемая организация. Например, целостность информации, передаваемой на бумажном носителе извне, получатель обеспечить не может.

Особое внимание нужно обратить на доступность информации.

*Пример:*



1. Определить угрозы безопасности информации.

На каждое свойство информации для каждого потока необходимо придумать не менее чем по одной угрозе безопасности информации. Минимальное общее количество угроз безопасности информации – 10, при этом следует помнить, что необходимо покрыть все свойства информации на каждом потоке.

Угрозы безопасности информации нужно представить в виде:

*УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы]. (Свойство информации: компонент 1 → компонент 2)*

1. Построить модель нарушителя.

Составить таблицу вида:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Нарушитель | Тип | Вид | Потенциал | Цели | Способы реализации |
| Бывший сотрудник | Внешний | Бывшие работники(пользова-тели) | Нарушители с базовым (низким) потенциалом | Месть за ранее совершен-ныедействия | НСД и (или) воздействие наобъекты на прикладном уровне |
| … | … | … | … | … | … |

Тип, вид, потенциал и цели должны быть указаны согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК (согласно таблицам 1 и 2 Методики).

Потенциал нарушителя будет являться первым критерием оценки возможной реализации угрозы безопасности информации.

1. Определить уровень проектной защищенности.

Уровень проектной защищенности будет вторым критерием оценки возможной реализации угрозы безопасности информации.

Согласно таблице 3 Методики определения угроз безопасности информации в информационных системах, разработанной ФСТЭК, необходимо определить показатели для вашего объекта информатизации, характеризующие проектную защищенность информационной системы. При расчете проектной защищенности это может быть отражено в виде краткой таблицы с количеством «+» для каждого уровня и выводом, но в отчете должен быть раздел с подробной таблицей.

*Пример:*

|  |  |  |
| --- | --- | --- |
| *Высокий* | *Средний* | *Низкий* |
| *+**+* | *+**+**+**+**+* | *+**+**+**+**+**+* |

*«+» в высоком и среднем уровне: 2 + 5 = 7*

*«+» всего: 2 + 5 + 6 = 13*

*7/13 < 9/10 → уровень проектной защищенности: низкий*

1. Определить актуальность угроз.

Необходимо составить таблицу вида:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Уровень проектной защищенности | Потенциал нарушителя | Возможность реализации угрозы | Степень ущерба | Актуальность угрозы |
| 1 | н | в | в | в | + |
| … | … | … | … | … | … |

Уровень проектной защищенности был определен в п.6, потенциал нарушителя – в п. 5. С их помощью необходимо определить возможность реализации угрозы.

Согласно таблице 7 Методики, необходимо обоснованно определить степень ущерба, который в совокупности с возможностью реализации угрозы позволит определить актуальность угрозы.

1. Определить для актуальных угроз меры защиты информации.

Составить для актуальных угроз таблицу вида:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ребро | Свойство | Угроза | Категория мер защиты | Подробно |
| Сервер → Банк | Целостность | УБИ1 | Организационные | Проведение статического анализа кодаРазвертывание тестовой среды |
| … | … | … | … | … |

1. Составить итоговый список всех мер.

Все меры, указанные в таблице п.8, нужно объединить по категориям и выделить в отдельный список.

*Пример:*

*Организационные:*

* *Развертывание тестовой среды*
* *…*

*Технические:*

* *Использование пленки для защиты визуальной информации на экранах и мониторах*
* *…*

*Криптографические:*

* *Шифрование передаваемых данных*
* *…*
1. Подготовиться к защите курсовой работы.

К моменту защиты работы необходимо свободно владеть понятиями, используемыми в работе, уметь приводить примеры и объяснять свою позицию.

**Критерии оценки работы:**

 Работы, не соответствующие формальным минимальным требованиям к численным параметрам рассматриваемого объекта, идентифицированных угроз, элементам отчета, считаются не выполненными и оцениваются 0 баллов.

При оценивании выполненной работы используются следующие промежуточные оценки, каждая из которых определяется по 10-балльной шкале:

|  |  |
| --- | --- |
| Оотчет | Оценивается оформление отчета, наличие титульного листа, введения с описанием объекта информатизации, таблиц, форматирования и т. д. |
| Ообъект | Оценивается соблюдение логики при моделировании объекта информатизации, корректность определения рассматриваемых свойств информации. |
| Омодель нарушителя | Оценивается корректность построения модели нарушителя – соответствие методике ФСТЭК и логике рассматриваемого объекта. |
| Омодель угроз | Оценивается корректность описания угроз безопасности информации, определения их свойств, оценки актуальности угроз. |
| Омеры защиты | Оценивается корректность выбора мер защиты для всех актуальных угроз объекта информатизации, а также их полнота – покрытие всех актуальных угроз.  |

 *Итоговая оценка за курсовую работу определяется по формуле:*

*Оитог = 0,1 \** Оотчет + 0, 15 \* Ообъект + 0, 2 \* Омодель нарушителя +

+ 0, 2 \* Омодель угроз + 0, 35 \* Омеры защиты

Округление в итоговой оценке за курсовую работу – арифметическое.