**Практическая работа №20. Оценка уязвимости информации**

**Цель работы:** Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

**Практическое задание:**

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»

2. Ознакомьтесь с **Приложениями C, D** и **Е** ГОСТа.

3. Выберите три различных информационных актива организации.

4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов, предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

**Ход работы**

1. Прочитал теоретические основы и ознакомились с ГОСТом Р ИСО/МЭК ТО 13335-3-2007
2. Информационные активы организации:

* информация/данные (например, файлы, содержащие информацию о платежах или продукте);
* аппаратные средства (например, компьютеры, принтеры);
* программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения);

1. Конкретные уязвимости системы защиты указанных информационных активов:

* Ошибки конфигурации аппаратной части и ПО встречаются весьма часто. Распространенными их причинами являются недостаточно качественная разработка и отсутствие тестов на корректную работу дополнительных функций. К этой категории также можно относить слишком простые пароли и оставленные без изменений учетные записи по умолчанию.
* Ошибки, допущенные при проектировании, сложнее всего обнаружить и устранить. Это — неточности алгоритмов, закладки, несогласованности в интерфейсе между разными модулями или в протоколах взаимодействия с аппаратной частью, внедрение неоптимальных технологий. Их устранение является весьма трудоемким процессом, в том числе потому, что они могут проявиться в неочевидных случаях — например, при превышении предусмотренного объема трафика или при подключении большого количества дополнительного оборудования, что усложняет обеспечение требуемого уровня безопасности и ведет к возникновению путей обхода межсетевого экрана.
* несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

1. Возможные угрозы:

* Хакерское ПО (имитация действий законного пользователя)
* Кража и мошенничество;
* Возможный вред со стороны персонала;

5. Оценка рисков информационной безопасности

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
| ***Ценность актива*** | ***Уровень угрозы*** | | | | | | | | |
|  | ***Низкий*** | | | ***Средний*** | | | ***Высокий*** | | |
|  | ***Уровень уязвимости*** | | | ***Уровень уязвимости*** | | | ***Уровень уязвимости*** | | |
|  | ***Н*** | ***С*** | ***В*** | ***Н*** | ***С*** | ***В*** | ***Н*** | ***С*** | ***В*** |
| ***0*** | ***0*** | ***1*** | ***2*** | ***1*** | ***2*** | ***3*** | ***2*** | ***3*** | ***4*** |
| ***1*** | ***1*** | ***2*** | ***3*** | ***2*** | ***3*** | ***4*** | ***3*** | ***4*** | ***5*** |
| ***2*** | ***2*** | ***3*** | ***4*** | ***3*** | ***4*** | ***5*** | ***4*** | ***5*** | ***6*** |
| ***3*** | ***3*** | ***4*** | ***5*** | ***4*** | ***5*** | ***6*** | ***5*** | ***6*** | ***7*** |
| ***4*** | ***4*** | ***5*** | ***6*** | ***5*** | ***6*** | ***7*** | ***6*** | ***7*** | ***8*** |
| **Обозначение: Н - низкий, С - средний, В - высокий.** | | | | | | | | | |

* В – необходимо выполнить корректирующее действие, а также рекомендуется внедрить меры и средства контроля и управления.
* С – требуется периодическй мониторинг.
* H – необходимо выполнить корректирующее действие и внедрить меры и средства контроля и управления.

**Контрольные вопросы:**

Дайте определение понятиям:

1. Уязвимости системы защиты информации - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

2. Угрозы ИБ - совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

3. Оценка рисков - выявление опасностей, существующих на производстве, определение масштабов этих опасностей и их возможных последствий; один из способов предупреждения несчастных случаев на производстве и повышения безопасности труда.