**Лабораторная работа № 2**

**Аттестация объектов информатизации по требованиям безопасности**

**Цель занятия:** изучить формы документации заполняемой при проведение аттестации объектов информатизации по требованиям безопасности, а также получить навыки их заполнения для заданной организации.

**1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

**Требования к нормативным и методическим документам по аттестации объектов информатизации**

Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.

Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены.

В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование. В них должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.

Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

При аттестации следует использовать стандартизованные количественные оценки состояния ИБ. Одной из таких методик является **общая система оценки уязвимостей** (Common Vulnerability Scoring System – CVSS) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности. В настоящее время наибольшее распространение в практической деятельности по оценке опасности уязвимостей получила версия 2.0 общей системы оценки уязвимостей. Система оценки CVSS v2.0 состоит из трех групп метрик (критериев): базовых, временных и контекстных. Группа базовых метрик (критериев) отражает аспекты опасности уязвимости, влияющие на доступность, целостность и конфиденциальность информации. Группа временных метрик (критериев) отражает характеристики уязвимости, которые изменяются со временем (подтверждение технических параметров уязвимости, статус исправления уязвимости и доступность технологии эксплуатации), но не зависят от среды функционирования программного обеспечения. Группа контекстных метрик (критериев) отражает характеристики уязвимости, зависящие от среды функционирования программного обеспечения.

**ЧАСТЬ 1. Калькулятор CVSS V3**

Выполнение заданий 1 – 3 предполагает о**формление отчета в электронном виде** в текстовом редакторе Word, в котором отражаются этапы выполнения заданий и результаты (ответы на вопросы, скриншоты заполненных полей калькулятора, документы аттестации ИБ и т.д.)

**Задание 1.** Изучение онлайн-калькулятора оценки ИБ

**1.1**. Перейти на сайт «Банк данных угроз безопасности информации» ФСТЭК (Федеральная служба по техническому и экспортному контролю):

<https://bdu.fstec.ru/threat>

и, далее, зайти на вкладку «**Уязвимости» - «Калькулятор CVSS V3.»** – калькулятор общей системы оценки уязвимостей версии 3 (CVSS - Common Vulnerability Scoring System – Общая система оценки уязвимостей).

**1.2.** Перед дальнейшей работой оставьте открытым сайт калькулятора и перейдите на сайт:

<https://www.first.org/cvss/v2/guide>

# где изучить представленный там материал «Полное руководство по общей системе оценки уязвимостей», после чего письменно (в электронном документе) ответить на вопросы:

1. Что такое CVSS?
2. Как работает CVSS?
3. Кто выполняет оценку?
4. Кто владеет CVSS?
5. Кто использует CVSS?
6. Перечислите метрические группы.
7. Перечислите и поясните базовые показатели
8. Перечислите и поясните временные показатели
9. Перечислите и поясните экологические показатели
10. Что содержит описание каждой метрика в векторе?

**1.3**. Выберете какое-либо программное обеспечение той организации, в которой Вы работаете (или учитесь), и с помощью калькулятора Калькулятор CVSS V3 рассчитайте значения всех метрик (базовых, временных и контекстных). Если смысл каких либо компонент вектора не понятен – воспользуйтесь справочником CVSS, нажав кнопку «Справочник CVSS» (она находится слева, под строкой меню в калькуляторе).

Рассчитываемое калькулятором значение автоматически появляется в строке напротив соответствующей метрики. При выборе уровня того или иного показателя надо уметь обосновать этот выбор!

**1.4.** Провести исследование влияния базовых показателей на базовую оценку. Варьируемые показатели представлены таблице 1. Надо выбрать показатели по варианту N, который выбирается в соответствии с номером в списке группы.

Таблица 1 – Варьируемые базовые показатели

|  |  |
| --- | --- |
| **Вариант** | **Показатель, который изменяется** |
| Четный N | AV, AC, Au. Остальные фиксируем как «частичное (Р)») |
| Нечетный N | С, I, A. Остальные фиксируем на уровнях смежная (А), средняя (М), единственная (N) |

Каждый из варьируемых показателей может принимать три значения. Перебрать все комбинации этих значений (их всего 27) и зафиксировать в таблице результатов для каждой комбинации результат (который обозначим как **R)**, выдаваемый калькулятором. Форму таблицы придумать самостоятельно.

**1.5.** Написать программу (в любой среде или на любом языке программирования), которая обрабатывала бы результаты пункта 1.4. Для прграммы:

входные данные: таблица результатов **R** из п. 1.4;

выходные данные:

– комбинация базовых показателей, при которых достигается максимум результата, выдаваемого калькулятором;

– трехмерные графикb **R(**AV, AC**), R(**AV, Au**), R(**AC, Au**)**.

Используя графики сделать вывод, как изменения показателей влияют на изменения **R.**

**1.6.** На основе данных п. 14.,1.5 предложите пути повышения ИБ – очевидно, что они должны приводить к увеличению значений в **R**. Результаты выполнения задания занесите в отчет по практическому занятию.

**ЧАСТЬ 2. Заполнение заявки на проведение аттестации**

**Задание 2.** Заполнить заявку на проведение аттестации (форма приведена в приложении А) объектов информатизации Вашего подразделения, предварительно ответив на вопросы и заполнив пункты исходных данных, представленных в приложении Б. В качестве подразделения можно выбрать свое место работы, а можно придумать произвольную организацию и для нее выполнит задание.

**Задание 3.** Заполнить аттестат соответствия, приведенный в приложении В, для своего подразделения.

**ПРИЛОЖЕНИЕ А. Форма заявки на аттестацию**

                                 Кому: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                        (наименование органа по аттестации

                                                    и его адрес)

                                  ЗАЯВКА

              на проведение аттестации объекта информатизации

    1.  (наименование  заявителя)  просит провести аттестацию (наименование

объекта   информатизации)   на  соответствие  требованиям  по  безопасности

информации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    2.  Необходимые  исходные данные по аттестуемому объекту информатизации

прилагаются (см. приложение Б).

    3.  Заявитель  готов  предоставить  необходимые документы и условия для

проведения аттестации.

    4.  Заявитель  согласен  на  договорной основе оплатить расходы по всем

видам  работ  и  услуг  по  аттестации  указанного  в данной заявке объекта

информатизации.

    5. Дополнительные условия или сведения для договора:

    5.1.  Предварительное  ознакомление  с  аттестуемым  объектом предлагаю

провести в период \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    5.2.  Аттестационные испытания объекта информатики предлагаю провести в

период \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    5.3.  Испытания  несертифицированных  средств  и  систем информатизации

(наименование  средств  и  систем)  предусмотрено  провести в испытательных

центрах   (лабораториях)  (наименование  испытательных  центров)  в  период

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (или предлагается провести непосредственно на аттестуемом

объекте в период \_\_\_\_\_).

    Другие условия (предложения).

Печать   Руководитель (органа заявителя)

    (подпись, дата) (Фамилия, И.О.)

**ПРИЛОЖЕНИЕ Б. Исходные данные по аттестуемому объекту информатизации**

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов:

1. Полное и точное наименование объекта информатизации и его назначение.

2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия)).

3. Организационная структура объекта информатизации.

4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).

5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

8. Наличие и характер взаимодействия с другими объектами информатизации.

9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.

10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

**ПРИЛОЖЕНИЕ В. Форма аттестата соответствия**

"УТВЕРЖДАЮ"

(должность руководителя органа по аттестации)

    м.п.                               Ф.И.О.

"\_\_" \_\_\_\_\_\_\_\_\_ 20\_\_ г.

                           АТТЕСТАТ СООТВЕТСТВИЯ

         (указывается полное наименование объекта информатизации)

                    ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

                                  N \_\_\_\_

                      Действителен до "\_\_" \_\_\_\_\_ 20\_\_ г.

    1.   Настоящим   АТТЕСТАТОМ  удостоверяется,  что:  (приводится  полное

наименование объекта информатизации) \_\_\_\_\_\_\_\_ категории \_\_\_\_\_\_\_\_\_\_\_\_ класса

соответствует   требованиям  нормативной  и  методической  документации  по

безопасности информации.

    Состав   комплекса   технических   средств  объекта  информатизации  (с

указанием  заводских  номеров, модели, изготовителя, номеров сертификатов),

схема  размещения  в  помещениях и относительно границ контролируемой зоны,

перечень  используемых  программных  средств,  а  также  средств  защиты (с

указанием изготовителя и номеров сертификатов) прилагаются.

    2.   Организационная   структура,   уровень   подготовки  специалистов,

нормативное,  методическое  обеспечение  и  техническая оснащенность службы

безопасности  информации  обеспечивают контроль эффективности мер и средств

защиты  и поддержание уровня защищенности объекта информатизации в процессе

эксплуатации в соответствии с установленными требованиями.

    3.   Аттестация  объекта  информатизации  выполнена  в  соответствии  с

программой    и    методиками   аттестационных   испытаний,   утвержденными

"\_\_" \_\_\_\_\_\_\_ 20\_\_ г. N \_\_\_\_\_\_.

    4.   С   учетом   результатов   аттестационных   испытаний  на  объекте

информатизации    разрешается   обработка   (указывается   высшая   степень

секретности, конфиденциальности) информации.

    5.  При  эксплуатации  объекта информатизации запрещается: (указываются

ограничения,  которые  могут повлиять на эффективность мер и средств защиты

информации).

    6.  Контроль  за  эффективностью  реализованных  мер  и  средств защиты

возлагается на службу безопасности информации.

    7. Подробные результаты аттестационных испытаний приведены в заключении

аттестационной  комиссии  (N \_\_\_\_\_\_\_ "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ г.)  и   протоколах

испытаний.

    8.  "Аттестат  соответствия"  выдан  на  \_\_\_\_\_  года, в течение которых

должна   быть  обеспечена  неизменность  условий  функционирования  объекта

информатизации   и  технологии  обработки  защищаемой  информации,  могущих

повлиять на характеристики, указанные в п. 9.

    9.  Перечень характеристик, об изменениях которых требуется обязательно

извещать орган по аттестации.

    9.1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    9.2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель аттестационной комиссии

(должность с указанием наименования предприятия)

Ф.И.О.

"\_\_" \_\_\_\_\_\_\_ 20\_\_ г.

Отметки органа надзора: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Примечание. Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.