**Лабораторная работа.**

**АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

**МАТРИЧНЫЙ ПОДХОД.**

Критичность актива

0 – не значителен;

1 – важен;

2 – очень важен;

3 – крайняя степень важности.

Уязвимость

0 – нет связи

1 – слабая связь

3 – умеренная связь

9 – сильная связь

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Активы** | | | | | | |
| Техническое оборудование | Интеллектуальная собственность | ПДн | Финансовые средства | Имущество |  | |
| Критичность актива | 2 | 3 | 3 | 3 | 2 |  | |
| **Уязвимость** |  |  |  |  |  | Всего | Приоритет уязвимости |
| Уязвимости рабочих станций | 1 | 9 | 9 | 3 | 0 | 65 | 3 |
| Уязвимости СЭД 1С | 0 | 0 | 9 | 1 | 0 | 30 | 6 |
| Отсутствие технической защиты | 3 | 9 | 9 | 3 | 3 | 75 | 2 |
| Отсутствие инструктажа персонала по ИБ | 1 | 9 | 9 | 1 | 3 | 65 | 3 |
| Уязвимость производственного сервера | 1 | 9 | 0 | 3 | 0 | 38 | 5 |
| Уязвимость сервера хранилища кода TFS. | 0 | 9 | 0 | 0 | 0 | 27 | 7 |
| Уязвимости СУБД PostgreSQL | 0 | 9 | 9 | 3 | 0 | 63 | 4 |
| Не декларированные возможности | 1 | 9 | 9 | 3 | 0 | 65 | 3 |
| Недостаточная физическая защита | 9 | 3 | 9 | 3 | 9 | 81 | 1 |

Таблица 1. Матрица активов (связь между активами и уязвимостью)

Угроза 0 – нет связи 1 – слабая связь 3 – умеренная связь 9 – сильная связь

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Уязвимости** | | | | | | | | | | |
| Уязвимости рабочих станций | Уязвимости СЭД 1С | Отсутствие технической защиты | Отсутствие инструктажа персонала по ИБ | Уязвимость производственного сервера | Уязвимость сервера хранилища кода TFS. | Уязвимости СУБД PostgreSQL | Недекларированные возможности | Недостаточная физическая защита |  | |
| Приоритет уязвимости | 3 | 6 | 2 | 3 | 5 | 7 | 4 | 3 | 1 |  | |
| **Угроза** |  | | | | | | | | | всего | Приоритет угрозы |
| Утечка программного кода | 3 | 0 | 1 | 1 | 3 | 9 | 0 | 0 | 0 | 92 | 1 |
| Утечка ПДн | 0 | 9 | 1 | 1 | 0 | 0 | 0 | 1 | 3 | 65 | 4 |
| Несанкционированный доступ к АРМ | 9 | 0 | 1 | 3 | 0 | 0 | 0 | 0 | 3 | 41 | 5 |
| Внедрение вредоносного ПО | 9 | 0 | 9 | 9 | 0 | 0 | 0 | 0 | 1 | 73 | 3 |
| Угроза использования не декларированных возможностей ПО | 1 | 1 | 0 | 0 | 3 | 3 | 3 | 9 | 0 | 84 | 2 |
| Отказ в обслуживании | 0 | 0 | 3 | 0 | 3 | 0 | 0 | 0 | 3 | 24 | 7 |
| Удаленный запуск приложений | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 9 | 8 |
| НСД к ПДн, в помещениях, предназначенных для хранения | 0 | 0 | 0 | 9 | 0 | 0 | 0 | 0 | 9 | 36 | 6 |

Таблица 2. Матрица активов (связь между угрозами и уязвимостями)

Контрмера 0 – нет связи 1 – слабое влияние 3 – умеренное влияние 9 – сильное влияние

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Угрозы** | | | | | | | | | |
| Утечка программного кода | Утечка ПДн | Несанкционированный доступ к АРМ | Внедрение вредоносного ПО | Угроза использования не декларированных возможностей ПО | Отказ в обслуживании | Удаленный запуск приложений | НСД к ПДн, в помещениях, предназначенных для хранения |  | |
| Приоритет угрозы | 1 | 4 | 5 | 3 | 2 | 7 | 8 | 6 |  | |
| **Контрмера** |  | | | | | | | | всего | Приоритет контрмеры |
| Использование ПАСЗИ | 0 | 3 | 9 | 3 | 9 | 9 | 3 | 9 | 225 | 1 |
| Настройка встроенных средств ИБ | 3 | 3 | 9 | 3 | 9 | 3 | 3 | 0 | 132 | 2 |
| Укрепление физической защиты | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 3 | 36 | 5 |
| Проведение инструктажей с персоналом | 9 | 9 | 0 | 3 | 0 | 0 | 0 | 3 | 69 | 3 |
| Использование метода минимальных полномочий | 3 | 3 | 0 | 0 | 0 | 0 | 0 | 3 | 33 | 6 |
| Использование парольных политик | 3 | 3 | 1 | 0 | 1 | 3 | 3 | 0 | 67 | 4 |

Таблица 3. Матрица угроз и контрмер.