|  |  |  |
| --- | --- | --- |
| v.1.2 – Добавил отчет ScanOval в приложение  v.2 – Отредактирован отчет полностью  Вставка из ПО  Результат ПО  Результат ПО |  | УТВЕРЖДАЮ  Ректор ДВГМУ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Ю.А. Давыдов  м.п.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 г. |

ОТЧЕТ

о результатах анализа защищенности информации системы защиты в информационной системе «ISName» федерального государственного бюджетного образовательного учреждения высшего образования «Дальневосточный государственный медицинский университет» Министерства здравоохранения Российской Федерации

DateReport комиссией в составе: Шматок В.А. – руководитель отдела информационных технологий, Хандожко Г.В. – ведущий специалист отдела информационных технологий, Ткаченко Е.Д. – администратор информационной безопасности был проведен анализ защищенности информационной системы (далее − ИС) «ISName1» федерального государственного бюджетного образовательного учреждения высшего образования «Дальневосточный государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее − Учреждение).

Целью анализа защищенности является выявление уязвимостей ИС «ISName2».

1. **Описание объекта информатизации**

Объектом аттестационных испытаний является ИС с входящими в её состав средствами вычислительной техники (СВТ), программными средствами, комплексом средств защиты информации от НСД и необходимой организационно-распорядительной, технической и эксплуатационной документацией. Объект состоит из NumOfWP NumOfServers

Объект размещен в кабинетах № NumsOfCabinets Учреждения по адресу: AddressOfComp.

Состав программного обеспечения, применяемого для обработки информации ограниченного доступа в ИС «ISName3», представлен в таблице 1.

Таблица 1 – Состав программных средств обработки информации ограниченного доступа в ИС «ISName4»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование АРМ | Наименование программных средств | Версия | Разработчик |
| 1 | АРМ 1 | Операционная система Microsoft Windows 7 Professional | 6.1.7601 | Microsoft Corporation |
| Офисный пакет прикладного ПО Microsoft Office профессиональный плюс 2010 | 14.0.7015.1000 | Microsoft Corporation |
| Интернет браузер Google Chrome | 49.0.2623.112 | Google Inc. |

Перечень программного обеспечения не был изменен и **соответствует** данным из технического паспорта.

Характеристика комплексов основных технических средств и систем в ИС «ISName5» представлены в таблице 2.

Таблица 2 – Состав технических средств обработки информации ограниченного доступа в ИС «ISName6»

| № п/п | Наименование элемента ИС | Инвентарный или заводской номер |
| --- | --- | --- |
| 1. АРМ 1 (кабинет № 100) в составе: | | |
| 1.1 | Системный блок | 1101040212075 |
| 1.2 | Монитор Philips HNS7190T | AU3A0710017547 |
| 1.3 | Клавиатура Microsoft RT2300 | 7668200926599 |
| 1.4 | Мышь Logitech M-SBF90 | 12075 |
| 5 | МФУ Xerox Phaser 3250 | 21011240219642 |
| 6 | МФУ Xerox Phaser 3250 | 21011240219641 |
| 7 | МФУ Xerox Phaser 3250 | 21011240219644 |
| 8 | МФУ Xerox WorkCentre 5021 | 21011240219616 |
| 9 | МФУ Canon MF6140dn | 2101340220774 |
| 19 | Коммутатор 3COM OfficeConnect Dual Speed Switch 16 | 2101040511580 |

Конфигурация ОТСС не изменилась и **соответствует** данным из технического паспорта.

Состав средств защиты информации, установленных в ИС «ISName7», представлен в таблице 3.

Таблица 3 – Состав средств защиты информации, установленных в ИС «ISName8»

| №  п/п | Наименование и тип  технического средства | Заводской номер  (№ лицензии) | Сведения о сертификате | Проверка соответствия |
| --- | --- | --- | --- | --- |
| 1. | Средство защиты информации «Secret Net Studio 8» (СЗИ от НСД) | 8A2XD5RB  H 440019 | Сертификат соответствия ФСТЭК России № 3745, действителен до 16.05.2020  (техническая поддержка  до 16.05.2025) | Сертификат действующий, Техническая поддержка производится |
| 2. | Средство защиты информации «Secret Net Studio 8» (Межсетевой экран) |
| 3. | Средство защиты информации «Secret Net Studio 8» (Средство обнаружения вторжений) |
| 4. | Средство антивирусной защиты «Kaspersky Security Endpoint 10 для Windows» | СМП8069-12505  М 269208 | Сертификат соответствия ФСТЭК России № 3025, действителен до 25.11.2019 (техническая поддержка до 01.11.2021) | Срок действия сертификата истек, Техническая поддержка производится |
| 5. | Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.р2» | SDFSFVD  М 610016 | Сертификат соответствия ФСТЭК России № 2688, действителен 01.08.2018 г.  (техническая поддержка до 01.08.2018) | Срок действия сертификата истек, Техническая поддержка не производится |
| 9. | Программный комплекс «ViPNet Coordinator (версия 4)» (Средство криптографической защиты информации) |  | Сертификат соответствия ФСБ России № СФ/124-3431, действителен до 31.03.2021г.  (техническая поддержка до 01.03.2019) | Сертификат не найден |

1. **Результаты поиска уязвимостей**

Комиссией были проведены мероприятия по поиску уязвимостей в ИС «ISName9», в соответствии «Программой и методиками аттестационных испытаний системы защиты информации информационной системы персональных данных «ISName10» федерального государственного бюджетного образовательного учреждения высшего образования «Дальневосточный государственный медицинский университет» Министерства здравоохранения Российской Федерации» № 5/19/3-ПМ.

| Таблица 4 – Обнаруженные уязвимости | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IP-адрес | Количество уязвимостей по уровням опасности | | | | | | | |
| Критический | | Высокий | | Средний | | Низкий | |
| Сканер безопасности | ScanOval | Сканер-ВС | ScanOval | Сканер-ВС | ScanOval | Сканер-ВС | ScanOval | Сканер-ВС |
| Кол-во уязвимостей | - | 1 | 1 | 2 | 5 | 2 | 6 | 3 |
| Общее количество | 1 | | 3 | | 7 | | 9 | |

Полные отчеты анализа уязвимостей представлены в Приложениях А, Б.

Анализ защищенности выполнялся с помощью сканера безопасности «XSpider 7.8.25» версия 3.0. Результаты анализа уязвимостей приведены в Приложении А. В ходе проведения анализа защищенности выявлены уязвимости низкого и среднего уровня, которые не являются критичными для функционирования системы защиты информации информационной системы персональных данных «ISName11».

1. **Результат фиксации файлов СЗИ с помощью программы «ФИКС»**

Таблица Б1. Имена файлов в дистрибутиве СЗИ и их контрольные значения

|  |  |  |
| --- | --- | --- |
| Тип СЗИ | Наименование СЗИ | Результат тестирования |
| Средство защиты информации от несанкционированного доступа | «Secret Net Studio 8» | **Контрольные значения соответствуют исходным** |
| Средство антивирусной защиты | «Kaspersky Security Endpoint 10 для Windows» | **Контрольные значения не соответствуют исходным** |

Полный отчет фиксации файлов СЗИ с помощью программы «ФИКС» представлен в Приложении В.

1. **Проверка подсистемы управления потоками информации**

Для контроля реализованной в СЗИ объекта информатизации системы распределения доступа к информационным ресурсам и программным средствам, ее соответствия организационно-распорядительным документам использовались программные средства контроля эффективности СЗИ – средства проверки настроек системы защиты информации «Ревизор-1ХР» и «Ревизор-2ХР».

Была разработана подсистема разграничения доступа с помощью средства контроля защищенности от НСД «Ревизор 1 ХР» в соответствии с политикой безопасности и матрицей доступа, учитывающей мандатные правила разграничения доступа, принятые в аттестуемой ИС. Анализ результатов работы программы «Ревизор-2ХР» показал, что реальные права пользователей по доступу к защищаемым ресурсам соответствуют установленной разрешительной системе доступа, а примененные способы и средства защиты не позволяют получить несанкционированный доступ к защищаемым ресурсам ПЭВМ.

В ИС осуществляется управление потоками информации с помощью меток, соответствующих степени конфиденциальности.

С использованием штатных средств операционной системы производились попытки переноса информации в папку с другой категорией конфиденциальности. СЗИ от НСД запретила операцию копирования.

Полный отчет фиксации файлов СЗИ с помощью программы «Ревизор 2XP» представлен в Приложении Г.

1. **Результат проверки настроек СЗИ от НСД «Secret Net Studio 8»**

Настройки средства защиты информации от несанкционированного доступа «Secret Net Studio 8» **соответствуют** установленному уровню защищенности.

1. **Заключение**

По результатам проведения анализа защищённости комиссия подтверждает, что необходимый уровень защиты информации в ИС обеспечивается. Устранение выявленных уязвимостей возлагается на ответственного за защиту информации федерального государственного бюджетного образовательного учреждения высшего образования «Дальневосточный государственный медицинский университет» Министерства здравоохранения Российской Федерации.

|  |  |  |  |
| --- | --- | --- | --- |
| Руководитель отдела информационных технологий |  |  | Шматок В.А. |
|  |  |  |  |
| Ведущий специалист отдела информационных технологий |  |  | Хандожко Г.В. |
|  |  |  |  |
| Администратор информационной безопасности |  |  | Ткаченко Е.Д. |