МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

КУРГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Безопасность информационных автоматизированных систем»

**КОНТРОЛЬНАЯ РАБОТА**

**по дисциплине**

**«Методы проектирования защищенных распределенных ИС»**

Выполнили студенты гр. Т-40913 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/А.Ю.Бутенко/

подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.В.Пинигин/

подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/А.К.Марков/

подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Р.Д.Меньщиков/

подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/С.С.Коротких/

подпись

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.М.Мурадисинов/

подпись

Руководитель, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/С.В. Мельников/

подпись

Работа защищена с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2016 г.

**Оглавление**

[Постановка задачи 3](#_Toc467517506)

[Задача 1. Топология, оборудование. 4](#_Toc467517507)

[Задача 2. Список установленного ПО 6](#_Toc467517508)

[Задача 3. Модель угроз. 12](#_Toc467517509)

[Вероятность реализации угроз. 12](#_Toc467517510)

[Угрозы утечки информации по техническим каналам. 12](#_Toc467517511)

[Угрозы несанкционированного доступа к информации 13](#_Toc467517512)

[Возможность реализации угроз. 16](#_Toc467517513)

[Модель угроз для «Студента кафедры» 17](#_Toc467517514)

[Оценка опасности угроз 18](#_Toc467517515)

[Определение актуальности угроз. 20](#_Toc467517516)

[Модель угроз для «Внутреннего нарушителя» 22](#_Toc467517517)

[Оценка опасности угроз 24](#_Toc467517518)

[Определение актуальности угроз. 26](#_Toc467517519)

[Модель угроз для «Внешнего нарушителя» 28](#_Toc467517520)

[Оценка опасности угроз 30](#_Toc467517521)

[Определение актуальности угроз. 32](#_Toc467517522)

[Анализ модели угроз. 34](#_Toc467517523)

# Постановка задачи

1. Графически изобразить локальную сеть кафедры КГУ «БИАС» и перечислить всё оборудование.
2. Провести сравнительный анализ ПО на трех произвольно выбранных ПК.
3. Сформулировать модель угроз для ролей: «Студент», «Внутренний нарушитель», «Внешний нарушитель».

# Задача 1. Топология, оборудование.

C:\Users\Preacher\AppData\Local\Microsoft\Windows\INetCacheContent.Word\кафедра (1).png

Рис. 1. Графическое изображение топологии сети кафедры «БИАС»

Адреса сетей в аудиториях кафедры:

Г-205: 10.5.1.0/24

Г-207: 10.8.1.0/24

Г-208: 10.6.1.0/24

Г-209: 10.7.1.0/24

Г-210: 192.168.1.0/24

СПИСОК ОБОРУДОВАНИЯ В АУДИТОРИЯХ

Аудитория Г-205 оборудована:   
• ЭВМ на базе процессоров Intel Pentium с мониторами LCD 19", в количестве 7 штук.

Маршрутизатором беспроводным LINKSYS Wireless Broadband Router работающего в качестве WI-FI роутера

• Hub 16 PORT "SWITSHING";   
Аудитория Г-205а оборудована:   
• программно - аппаратным комплексом контроля и доступа видеонаблюдения, с помощью которого осуществляет видеонаблюдение на кафедре, а именно вход на кафедру и выход во двор;   
• ЭВМ на базе процессора AMD ATHLON 64 3200 с монитором ACER 17".   
Аудитория Г- 208 оборудована:   
• ЭВМ STORM: с CPU Intel Core i3 - 2120/PPR3 2Gb/320Gb/Rames Time 5013/ Monitor 21,5'', в количестве от 8 штук;   
• коммутационным шкафом 19";   
• коммутатором DGS -1016D D-Link   
Аудитория Г-209 оборудована:   
• ЭВМ STORM: с CPU Intel Core i3 - 2120/PPR3 2Gb/320Gb/Rames Time 5013/ Monitor 21,5'';   
• ЭВМ 3 с процессором Intel Core 2Duo E8600/Monitor 22", в количестве 2 штук;   
• ЭВМ с процессором AMD ATHLON64 3200+512 MB/17"/160GB.

Принтером HP DeskJet F4200 в количестве 1 штуки;

Маршрутизатором беспроводным LINKSYS   
Аудитория Г-210 оборудована:   
• ЭВМ на базе процессора Intel Core i серии с монитором 20", в количестве 11 штук.   
Аудитория Г-210а оборудована:   
• сервером 1 Intel Core специальный монитор 20" (серверная - шкаф) в количестве двух штук, один из которых неактивен.  
• коммутатором 3COM 8 портов, расположен в серверном шкафу;   
• ИБП UPS 425, в количестве трех штук;

ATM-коммутатором Cisco Lightstream 1010 в количестве трёх штук;  
• маршрутизатором беспроводным LINKSYS Wireless Broadband Router, расположен на серверном шкафу используется в качестве wi-fi роутера.

# Задача 2. Список установленного ПО

Таблица 1. Список ПО на компьютере n1 из аудитории 208.

|  |  |
| --- | --- |
| Name | Version |
| MPICH2 | 1.4.1 |
| Microsoft Application Error Reporting | 12.0.6012.5000 |
| MSXML 6.0 Parser (KB933579) | 6.10.1200.0 |
| MSXML 4.0 SP3 Parser (KB2758694) | 4.30.2117.0 |
| MSXML 4.0 SP3 Parser (KB2721691) | 4.30.2114.0 |
| Microsoft .NET Framework 3.0 Service Pack 2 | 3.2.30729 |
| Microsoft Visual C++ 2010 x86 Redistributable | 10.0.40219 |
| Microsoft Security Client | 4.4.0304.0 |
| Microsoft .NET Framework 3.5 SP1 | 3.5.30730 |
| Oracle VM VirtualBox 4.3.32 | 4.3.32 |
| Microsoft .NET Framework 3.0 Service Pack 2 Language Pack - RUS | 3.2.30729 |
| Disk Unlocker | 2.1.0 |
| LibreOffice 4.1 Help Pack (Russian) | 4.1.1.2 |
| Java 7 Update 15 | 7.0.150 |
| LibreOffice 4.1.1.2 SDK | 4.1.1.2 |
| Platform | 1.39 |
| MSXML 4.0 SP3 Parser (KB973685) | 4.30.2107.0 |
| Microsoft .NET Framework 4 Client Profile | 4.0.30319 |
| Adobe Reader XI (11.0.08) - Russian | 11.0.08 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 | 9.0.30729.6161 |
| WebFldrs XP | 9.50.7523 |
| Microsoft .NET Framework 1.1 Russian Language Pack | 1.1.4322 |
| Google Update Helper | 1.3.31.5 |
| LibreOffice 4.1.1.2 | 4.1.1.2 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729 | 9.0.30729 |
| Microsoft .NET Framework 2.0 Service Pack 2 Language Pack - RUS | 2.2.30729 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030 | 11.0.61030 |
| Microsoft Visual C++ 2005 Redistributable | 8.0.61001 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 | 9.0.30729.4148 |
| Microsoft Silverlight | 5.1.30514.0 |
| Microsoft .NET Framework 2.0 Service Pack 2 | 2.2.30729 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030 | 11.0.61030 |
| Microsoft .NET Framework 1.1 | 1.1.4322 |
| Microsoft .NET Framework 3.5 Language Pack SP1 - rus | 3.5.30729 |
| ASUS PC Diagnostics | 1.1.9 |
| Java Auto Updater | 2.1.9.0 |
| Microsoft .NET Framework 4 Extended | 4.0.30319 |

Таблица 2. Список ПО на компьютере n2 из аудитории 208.

|  |  |
| --- | --- |
| Name | Version |
| Пакет обеспечения совместимости для выпуска 2007 системы Microsoft Office | 12.0.6514.5001 |
| Microsoft Application Error Reporting | 12.0.6012.5000 |
| Microsoft Help Viewer 1.0 Language Pack - RUS | 1.0.30319 |
| MSXML 4.0 SP3 Parser (KB2758694) | 4.30.2117.0 |
| MSXML 4.0 SP3 Parser (KB2721691) | 4.30.2114.0 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.50727.4053 False | 8.0.50727.4053 |
| Microsoft .NET Framework 3.0 Service Pack 2 | 3.2.30729 |
| LibreOffice 5.1.3.2 | 5.1.3.2 |
| Microsoft Visual C++ 2010 Redistributable - x86 10.0.40219 | 10.0.40219 |
| Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 | 12.0.21005 |
| Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 | 12.0.21005 |
| Microsoft Security Client | 4.4.0304.0 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022.0 False | 9.0.21022 |
| Microsoft .NET Framework 3.5 SP1 | 3.5.30729 |
| Microsoft .NET Framework 4 Client Profile RUS Language Pack | 4.0.30319 |
| Microsoft SQL Server 2008 Common Files | 10.1.2531.0 |
| Microsoft SQL Server 2008 Database Engine Services | 10.1.2531.0 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4048 False | 9.0.30729.4048 |
| Oracle VM VirtualBox 4.3.40 | 14674 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.59193 False | 8.0.59193 |
| Microsoft .NET Framework 3.0 Service Pack 2 Language Pack - RUS | 3.2.30729 |
| Microsoft SQL Server VSS Writer | 10.1.2531.0 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.57103 False | 8.0.57103 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.60610 False | 11.0.60610 |
| LibreOffice 4.1 Help Pack (Russian) | 4.1.1.2 |
| Java 7 Update 101 | 7.0.1010 |
| Java(TM) 6 Update 30 | 6.0.300 |
| LibreOffice 4.1.1.2 SDK | 4.1.1.2 |
| Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23026 False | 14.0.23026 |
| Platform | 14246 |
| MSXML 4.0 SP3 Parser (KB973685) | 4.30.2107.0 |
| Microsoft .NET Framework 4 Client Profile | 4.0.30319 |
| Adobe Reader XI (11.0.08) - Russian | 11.0.08 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.51106 False | 11.0.51106 |
| Microsoft SQL Server 2008 Database Engine Shared | 10.1.2531.0 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.5570 False | 9.0.30729.5570 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 | 9.0.30729.6161 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 False | 9.0.21022 |
| Microsoft SQL Server 2008 Database Engine Shared | 10.1.2531.0 |
| tools-winPre2k | 9.2.0.812388 |
| tools-netware | 9.2.0.812388 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.60610 False | 11.0.60610 |
| Microsoft SQL Server 2008 Browser | 10.1.2531.0 |
| Microsoft .NET Framework 4 Multi-Targeting Pack | 4.0.30319 |
| WebFldrs XP | 9.50.7523 |
| Microsoft SQL Server 2008 Common Files | 10.0.1600.22 |
| Microsoft HPC Pack 2008 R2 MS-MPI Redistributable Pack | 3.4.4169.0 |
| Microsoft SQL Server 2008 RsFx Driver | 10.1.2531.0 |
| Microsoft .NET Framework 1.1 Russian Language Pack | 884619 |
| Microsoft SQL Server 2008 Native Client | 10.1.2531.0 |
| Google Update Helper | 1.3.31.5 |
| tools-linux | 9.2.0.812388 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.58299 False | 8.0.58299 |
| Microsoft Help Viewer 1.0 | 1.0.30319 |
| VMware Workstation | 9.0.0 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.56336 False | 8.0.56336 |
| SharpDevelop 4.3 alpha | 2716738 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729 False | 9.0.30729 |
| IIS 7.5 Express | 7.5.1190 |
| tools-solaris | 9.2.0.812388 |
| Microsoft .NET Framework 2.0 Service Pack 2 Language Pack - RUS | 2.2.30729 |
| Application Verifier | 4.0.665 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030 | 11.0.61030 |
| Sql Server Customer Experience Improvement Program | 10.1.2531.0 |
| Microsoft SQL Server 2008 Database Engine Services | 10.1.2531.0 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.51106 False | 11.0.51106 |
| Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23026 False | 14.0.23026 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.61001 | 8.0.61001 |
| tools-windows | 9.2.0.812388 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 False | 9.0.30729.4148 |
| Microsoft Visual C++ 2010 Redistributable - x86 10.0.30319 False | 10.0.30319 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 False | 9.0.30729 |
| Microsoft Silverlight | 5.1.30514.0 |
| Файлы поддержки программы установки Microsoft SQL Server 2008 | 10.1.2731.0 |
| Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23506 | 14.0.23506 |
| tools-freebsd | 9.2.0.812388 |
| Microsoft .NET Framework 2.0 Service Pack 2 | 2.2.30729 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30411 False | 9.0.30411 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030 | 11.0.61030 |
| Microsoft .NET Framework 1.1 | 884619 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148.0 False | 9.0.30729.4148 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.51011 False | 8.0.51011 |
| Microsoft SQL Server Compact 3.5 SP2 RUS | 3.5.8080.0 |
| X86 Debuggers And Tools | 8.100.25984 |
| Microsoft Visual C++ 2010 Express - RUS | 10.0.30319 |
| Microsoft .NET Framework 3.5 Language Pack SP1 - rus | 3.5.30729 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.0 False | 9.0.30729 |
| Java Auto Updater | 2.1.101.14 |
| Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23506 | 14.0.23506 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.50727.42 False | 8.0.50727.42 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022.218 False | 9.0.21022.218 |
| Microsoft .NET Framework 4 Extended | 4.0.30319 |
| Microsoft .NET Framework 4 Extended RUS Language Pack | 4.0.30319 |

Таблица 3. Список ПО на компьютере n3 из аудитории 208.

|  |  |
| --- | --- |
| Name | Version |
| Пакет обеспечения совместимости для выпуска 2007 системы Microsoft Office | 12.0.6514.5001 |
| Microsoft Application Error Reporting | 12.0.6012.5000 |
| Microsoft Help Viewer 1.0 Language Pack - RUS | 1.0.30319 |
| MSXML 4.0 SP3 Parser (KB2758694) | 4.30.2117.0 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.50727.4053 False | 8.0.50727.4053 |
| Microsoft .NET Framework 3.0 Service Pack 2 | 3.2.30729 |
| LibreOffice 5.1.3.2 | 5.1.3.2 |
| Microsoft Visual C++ 2010 Redistributable - x86 10.0.40219 | 10.0.40219 |
| Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 | 12.0.21005 |
| Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 | 12.0.21005 |
| Microsoft Security Client | 4.4.0304.0 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022.0 False | 9.0.21022 |
| Microsoft .NET Framework 3.5 SP1 | 3.5.30730 |
| Microsoft .NET Framework 4 Client Profile RUS Language Pack | 4.0.30319 |
| Microsoft SQL Server 2008 Common Files | 10.1.2531.0 |
| Microsoft SQL Server 2008 Database Engine Services | 10.1.2531.0 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4048 False | 9.0.30729.4048 |
| Oracle VM VirtualBox 4.3.40 | 14674 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.59193 False | 8.0.59193 |
| Microsoft .NET Framework 3.0 Service Pack 2 Language Pack - RUS | 3.2.30729 |
| Microsoft SQL Server VSS Writer | 10.1.2531.0 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.57103 False | 8.0.57103 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.60610 False | 11.0.60610 |
| Disk Unlocker | 36527 |
| Java 7 Update 101 | 7.0.1010 |
| Java 8 Update 60 | 8.0.600.27 |
| Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23026 False | 14.0.23026 |
| Platform | 14246 |
| MSXML 4.0 SP3 Parser (KB973685) | 4.30.2107.0 |
| Microsoft .NET Framework 4 Client Profile | 4.0.30319 |
| Adobe Reader XI (11.0.08) - Russian | 11.0.08 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.51106 False | 11.0.51106 |
| Microsoft SQL Server 2008 Database Engine Shared | 10.1.2531.0 |
| LibreOffice 4.4 Help Pack (Russian) | 4.4.5.2 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.5570 False | 9.0.30729.5570 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 | 9.0.30729.6161 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 False | 9.0.21022 |
| Microsoft SQL Server 2008 Database Engine Shared | 10.1.2531.0 |
| Microsoft .NET Framework 2.0 Language Pack - RUS | 1.1.50727.42 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.60610 False | 11.0.60610 |
| Microsoft SQL Server 2008 Browser | 10.1.2531.0 |
| Microsoft .NET Framework 4 Multi-Targeting Pack | 4.0.30319 |
| WebFldrs XP | 9.50.7523 |
| Microsoft SQL Server 2008 Common Files | 10.0.1600.22 |
| Microsoft HPC Pack 2008 R2 MS-MPI Redistributable Pack | 3.4.4169.0 |
| Microsoft SQL Server 2008 RsFx Driver | 10.1.2531.0 |
| PGP Desktop | 10.1.2.9 |
| Microsoft .NET Framework 1.1 Russian Language Pack | 884619 |
| Microsoft SQL Server 2008 Native Client | 10.1.2531.0 |
| LibreOffice 4.4.5.2 SDK | 4.4.5.2 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.58299 False | 8.0.58299 |
| Microsoft Help Viewer 1.0 | 1.0.30319 |
| VMware Player | 3.1.3.14951 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.56336 False | 8.0.56336 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729 False | 9.0.30729 |
| Microsoft .NET Framework 2.0 Service Pack 2 Language Pack - RUS | 2.2.30729 |
| Application Verifier | 4.0.665 |
| Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030 | 11.0.61030 |
| Sql Server Customer Experience Improvement Program | 10.1.2531.0 |
| Microsoft SQL Server 2008 Database Engine Services | 10.1.2531.0 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.51106 False | 11.0.51106 |
| Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23026 False | 14.0.23026 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.61001 | 8.0.61001 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 False | 9.0.30729.4148 |
| Microsoft Visual C++ 2010 Redistributable - x86 10.0.30319 False | 10.0.30319 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 False | 9.0.30729 |
| Microsoft Silverlight | 5.1.30514.0 |
| Файлы поддержки программы установки Microsoft SQL Server 2008 | 10.1.2731.0 |
| Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23506 | 14.0.23506 |
| Microsoft .NET Framework 2.0 Service Pack 2 | 2.2.30729 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30411 False | 9.0.30411 |
| Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030 | 11.0.61030 |
| Microsoft .NET Framework 1.1 | 884619 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148.0 False | 9.0.30729.4148 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.51011 False | 8.0.51011 |
| Microsoft SQL Server Compact 3.5 SP2 RUS | 3.5.8080.0 |
| Microsoft Visual C++ 2010 Express - RUS | 10.0.30319 |
| Microsoft .NET Framework 3.5 Language Pack SP1 - rus | 3.5.30729 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.0 False | 9.0.30729 |
| ASUS PC Diagnostics | 39814 |
| Java Auto Updater | 2.8.60.27 |
| Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23506 | 14.0.23506 |
| Microsoft Visual C++ 2005 Redistributable - x86 8.0.50727.42 False | 8.0.50727.42 |
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022.218 False | 9.0.21022.218 |
| Microsoft .NET Framework 4 Extended | 4.0.30319 |
| Microsoft .NET Framework 4 Extended RUS Language Pack | 4.0.30319 |

Из данных таблиц можно сделать вывод, что первый ОС на компьютере n1 была недавно переустановлена. Остальные 2 имеют минимальные отличия в списке установленного ПО. В основном это необходимые для работы библиотеки или наборы утилит (Microsoft redistributable, Microsoft framework). Кроме них в списке встречаются программы необходимые для работы в учебном заведении (офис, пакеты для работы с ним, разного рода reader’ы).

Список информации, подлежащей к защите:

1. Методические указания
2. Отчеты по лабораторным работам

# Задача 3. Модель угроз.

## Вероятность реализации угроз.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для ИС кафедры в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

**маловероятно -** отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

**низкая вероятность**- объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

**средняя вероятность** *-* объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ИС недостаточны (Y2 = 5);

**высокая вероятность** *-* объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ИС не приняты (Y2 = 10).

Определение вероятности реализации угроз безопасности персональных данных проводится для всех выявленных угроз. Ниже приведен список всех выявленных угроз и их описание, а также предпринимаемые меры по их противодействию.

## Угрозы утечки информации по техническим каналам.

1.1 Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИС, при обработке данных в ИС, возможно при наличии функций голосового ввода данных в ИС или функций воспроизведения данных акустическими средствами ИС.

В ИС подразделений редакции функции голосового ввода или функции воспроизведения данных акустическими средствами отсутствуют.

Вероятность реализации угрозы для всех типов нарушителей – маловероятна(Y2 = 0)

1.2 Угрозы утечки видовой информации.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС.

На кафедре введен пропускной режим, который исключает возможность проникновения посторонних.

Вероятность реализации угрозы для внешнего нарушителя - маловероятна. (Y2 = 0)

Вероятность реализации угрозы для студентов кафедры и внутренних нарушителей - низкая. (Y2 = 2)

## Угрозы несанкционированного доступа к информации

2.1 Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС.

2.1.1 Кража ПЭВМ.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены ПЭВМ.

Во всех аудиториях кафедры введен контроль доступа в контролируемую зону, двери закрываются на замок, установлена охранная сигнализация.

Вероятность реализации угрозы – маловероятна для всех нарушителей. (Y2 = 0).

2.1.2 Кража носителей информации.

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации и их последующей кражей.

На кафедре введен контроль доступа в контролируемую зону, двери закрываются на замок, установлена охранная сигнализация, ведется учет носителей.

Вероятность реализации угрозы - маловероятна. (Y2 = 0).

2.1.3 Кража ключей и атрибутов доступа.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

На кафедре введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, организовано хранение ключей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы - маловероятна. (Y2 = 0).

2.1.4 Кражи, модификации, уничтожения информации.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены ПЭВМ и средства защиты, а также происходит работа пользователей.

На кафедре введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы для внешнего нарушителя - маловероятна. (Y2 = 0)

Вероятность реализации угрозы для студентов кафедры и внутренних нарушителей - низкая. (Y2 = 2)

2.1.5 Вывод из строя узлов ПЭВМ, каналов связи.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены ПЭВМ и проходят каналы связи.

На кафедре введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы - маловероятна. (Y2 = 0)

**2.1.6 Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.**

Угроза осуществляется путем непреднамеренного или намеренного доступа к информации для лиц, не имеющих для этого прав во время технического обслуживания узлов ПЭВМ.

На кафедре администратор безопасности информации проинструктирован о порядке действий и применяемых мерах в случае ремонта, модернизации или замены узла ПЭВМ. Например, гарантированное удаление данных с устройств памяти ПЭВМ сертифицированными средствами и составление об этом акта или опечатывание устройств, в случае невозможности удаления данных.

Вероятность реализации угрозы – маловероятна (Y2 = 0).

2.1.7 Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты.

На кафедре введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери и электрические щитки закрываются на замок, пользователи проинструктированы о работе в ИС.

Вероятность реализации угрозы - маловероятна. (Y2 = 0)

**2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств.**

2.2.1 Действия вредоносных программ (вирусов).

Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера и выполнять без инициирования со стороны пользователя деструктивные функции (копирования, уничтожения, блокирования и т.п.);

- обладать способностью к самодублированию и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

- разрушать (искажать произвольным образом) код программ в оперативной памяти;

-На кафедре на всех элементах ПЭВМ установлена лицензионная и сертифицированная антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения и об установленной политике прав запуска приложений.

Вероятность реализации угрозы для внешнего нарушителя - маловероятна. (Y2 = 0)

Вероятность реализации угрозы для студентов кафедры и внутренних нарушителей - низкая. (Y2 = 2)

2.2.2 Недокументированные возможности системного ПО и ПО для обработки персональных данных.

Недокументированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Перед работой с ЭВМ в обязательном порядке предоставлять правила пользования, в которых будет указана также мера наказания при их нарушении в зависимости от типа нарушения. В качестве подтверждения своей ознакомленности, пользователь расписывается в бланке напротив своей фамилии.

Вероятность реализации угрозы – средняя (Y2 = 5).

## Возможность реализации угроз.

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y). Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если , то возможность реализации угрозы признается низкой;

если , то возможность реализации угрозы признается средней;

если , то возможность реализации угрозы признается высокой;

если , то возможность реализации угрозы признается очень высокой.

# Модель угроз для «Студента кафедры»

Таблица 3. Возможность реализации угроз.

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ИС | Y | Вербальная интерпретация |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации | Y = (0+ 0)/20 = 0 | Низкая |
| 1.2. Угрозы утечки видовой информации | Y = (2 + 0)/20 = 0,1 | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | | |
| 2.1.1. Кража ПЭВМ | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.2. Кража носителей информации | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Y = (2 + 0)/20 = 0,1 | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ. | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.7.Несанкционированное отключение средств защиты | Y = (0 + 0)/20 = 0 | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | | |
| 2.2.1. Действия вредоносных программ (вирусов) | Y = (2 + 0)/20 = 0,1 | Низкая |
| 2.2.2.Недокументированные возможности системного ПО и ПО для обработки персональных данных | Y = (5 + 0)/20 = 0,4 | Средняя |

## Оценка опасности угроз

Оценка опасности УБИС производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

**низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

**средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

**высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБИС представлена таблице.

Таблица 4 – Опасность УБИС

|  |  |
| --- | --- |
| Тип угроз безопасности ИС | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Низкая |
| 2.1.2. Кража носителей информации | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Низкая |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Средняя |

## Определение актуальности угроз.

Правила отнесения угрозы безопасности ИС к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Таблица 5.Актуальность угроз.

|  |  |
| --- | --- |
| Угроза | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Неактуальная |
| 1.2. Угрозы утечки видовой информации | Неактуальная |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Неактуальная |
| 2.1.2. Кража носителей информации | Неактуальная |
| 2.1.3. Кража ключей и атрибутов доступа | Неактуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | Неактуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Неактуальная |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Неактуальная |
| 2.1.7. Несанкционированное отключение средств защиты | Неактуальная |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Неактуальная |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Актуальная |

По итогам составленного перечня актуальности угроз, вероятности реализации, возможности реализации и их опасности, получаем частную модель угроз безопасности персональных данных для рассматриваемой кафедры. Данная модель угроз представлена в таблице.

# Модель угроз для «Внутреннего нарушителя»

Таблица 1. Возможность реализации угроз.

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ИС | Y | Вербальная интерпретация |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации | Y = (0+ 0)/20 = 0 | Низкая |
| 1.2. Угрозы утечки видовой информации | Y = (2 + 0)/20 = 0,1 | Низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Y = (0 + 0)/20 = 0 | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | | |
| 2.1.1. Кража ПЭВМ | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.2. Кража носителей информации | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Y = (2 + 0)/20 = 0,1 | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ. | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.7.Несанкционированное отключение средств защиты | Y = (0 + 0)/20 = 0 | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | | |
| 2.2.1. Действия вредоносных программ (вирусов) | Y = (2 + 0)/20 = 0,1 | Низкая |
| 2.2.2.Недокументированные возможности системного ПО и ПО для обработки персональных данных | Y = (0 + 0)/20 = 0 | Низкая |

## Оценка опасности угроз

Оценка опасности УБИС производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

**низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

**средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

**высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБИС представлена таблице.

Таблица 2 – Опасность УБИС

|  |  |
| --- | --- |
| Тип угроз безопасности ИС | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Низкая |
| 2.1.2. Кража носителей информации | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Низкая |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Низкая |

## Определение актуальности угроз.

Правила отнесения угрозы безопасности ИС к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Таблица 3.Актуальность угроз.

|  |  |
| --- | --- |
| Угроза | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Неактуальная |
| 1.2. Угрозы утечки видовой информации | Неактуальная |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Неактуальная |
| 2.1.2. Кража носителей информации | Неактуальная |
| 2.1.3. Кража ключей и атрибутов доступа | Неактуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | Неактуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Неактуальная |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Неактуальная |
| 2.1.7. Несанкционированное отключение средств защиты | Неактуальная |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Неактуальная |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Неактуальная |

По итогам составленного перечня актуальности угроз, вероятности реализации, возможности реализации и их опасности, получаем частную модель угроз безопасности персональных данных для рассматриваемой организации кафедры. Данная модель угроз представлена в таблице.

# Модель угроз для «Внешнего нарушителя»

Таблица 1. Возможность реализации угроз.

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ИС | Y | Вербальная интерпретация |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации | Y = (0 + 0)/20 = 0 | Низкая |
| 1.2. Угрозы утечки видовой информации | Y = (0 + 0)/20 = 0 | Низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Y = (0 + 0)/20 = 0 | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | | |
| 2.1.1. Кража ПЭВМ | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.2. Кража носителей информации | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ. | Y = (0 + 0)/20 = 0 | Низкая |
| 2.1.7.Несанкционированное отключение средств защиты | Y = (0 + 0)/20 = 0 | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | | |
| 2.2.1. Действия вредоносных программ (вирусов) | Y = (0 + 0)/20 = 0 | Низкая |
| 2.2.2.Недокументированные возможности системного ПО и ПО для обработки персональных данных | Y = (0 + 0)/20 = 0 | Низкая |

## Оценка опасности угроз

Оценка опасности УБИС производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

**низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

**средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

**высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБИС представлена таблице.

Таблица 2 – Опасность УБИС

|  |  |
| --- | --- |
| Тип угроз безопасности ИС | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ, носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Низкая |
| 2.1.2. Кража носителей информации | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Низкая |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Низкая |

## Определение актуальности угроз.

Правила отнесения угрозы безопасности ИС к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Таблица 3.Актуальность угроз.

|  |  |
| --- | --- |
| Угроза | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Неактуальная |
| 1.2. Угрозы утечки видовой информации | Неактуальная |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ПЭВМ носителей информации путем физического доступа к элементам ПЭВМ | |
| 2.1.1. Кража ПЭВМ | Неактуальная |
| 2.1.2. Кража носителей информации | Неактуальная |
| 2.1.3. Кража ключей и атрибутов доступа | Неактуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | Неактуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Неактуальная |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Неактуальная |
| 2.1.7. Несанкционированное отключение средств защиты | Неактуальная |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | Неактуальная |
| 2.2.2. Недокументированные возможности системного ПО и ПО для обработки персональных данных | Неактуальная |

По итогам составленного перечня актуальности угроз, вероятности реализации, возможности реализации и их опасности, получаем частную модель угроз безопасности персональных данных для рассматриваемой кафедры. Данная модель угроз представлена в таблице.

# Анализ модели угроз.

Таким образом, актуальными угрозами безопасности ИС, являются:

* недокументированные возможности системного ПО и ПО для обработки персональных данных.