ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Направление 10.03.01 «Информационная безопасность»

Дисциплина:

«Организация и управление службой защиты информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 4**

**Выполнил:** Лукина Д.С.

Студент гр. N3464

**Проверил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Канжелев Ю.А.

**Кол-во баллов:**

Санкт-Петербург

2019 г.

Задание: обеспечение ИБ при сетевом варианте мониторинга и обеспечения ИБ.

В ходе мониторинга за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

* контроль за событиями безопасности и действиями пользователей;
* контроль защищенности информации;
* анализ и оценка функционирования системы защиты информации, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации;
* периодический анализ изменения угроз безопасности информации и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
* документирование процедур и результатов мониторинга за обеспечением уровня защищенности информации.

При мониторинге контролируются следующие события:

* очистка журнала аудита;
* вход с учётной записью выполнен успешно;
* учётной записи не удалось выполнить вход в систему;
* создана учётная запись пользователя;
* попытка сбросить пароль учётной записи;
* отключена учётная запись пользователя;
* удалена учётная запись пользователя;
* создана защищённая группа безопасности;
* добавлен участник в защищённую группу;
* удален участник из защищённой группы;
* удалена защищённая группа безопасности;
* изменена защищённая группа безопасности;
* изменена учётная запись пользователя;
* заблокирована учётная запись пользователя;
* имя учётной записи было изменено.

описать работу сотрудника безопасности (обеспечение защиты от ВВК, контроль целостности, передача информации, обеспечение антивирусной безопасности)

.

Вывод: в результате лабораторной работы