Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

|  |  |  |  |
| --- | --- | --- | --- |
| Институт: | *ИнЭИ* | Кафедра: | *БИТ* |
| Направление подготовки: | | *10.03.01 Информационная безопасность* | |

**ОТЧЕТ по практике**

|  |  |
| --- | --- |
| **Наименование практики:** | Производственная практика: эксплуатационная практика |

**СТУДЕНТ**

|  |  |
| --- | --- |
|  | / Скальский Е.М. / |
| *(подпись )* | (*Фамилия и инициалы*) |

|  |  |
| --- | --- |
| Группа | ИЭ-45-20 |
|  | *(номер учебной группы)* |

**ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ПРАКТИКЕ**

|  |
| --- |
|  |
| *(отлично, хорошо, удовлетворительно, неудовлетворительно)* |

|  |  |
| --- | --- |
|  | / Артёмов А.С. / |
| *(подпись )* | (*Фамилия и инициалы члена комиссии*) |

|  |  |
| --- | --- |
|  | / Баронов О. Р. / |
| *(подпись )* | (*Фамилия и инициалы члена комиссии*) |

**Москва**

**2023**

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

|  |  |  |  |
| --- | --- | --- | --- |
| Институт: | *ИнЭИ* | Кафедра: | *БИТ* |
| Направление подготовки/специальность: | | *10.03.01 Информационная безопасность*  *Безопасность автоматизированных систем* | |

**ЗАДАНИЕ НА ПРАКТИКУ**

|  |  |  |
| --- | --- | --- |
| **Наименование практики:** | Производственная практика: эксплуатационная практика | |
| **Студент:** | *Скальский Егор Максимович* | |
|  | *(Фамилия, имя, отчество (при наличии) полностью)* | |
| **Группа:** | *ИЭ-45-20* | |
|  | *(номер учебной группы)* | |
| **Место прохождения практики:** | *НИУ МЭИ, ИнЭИ, Кафедра БИТ* | |
|  | *(наименование предприятия, организации, учреждения, подразделения МЭИ в соответствии с приказом о направлении на практику)* | |
| **Сроки практики:** | *15.06.2023 - 12.07.2023* | |
|  | *(в соответствии с приказом о направлении на практику)* | |
| **Содержание задания:** | |  |
| 1. Вводный инструктаж на кафедре БИТ | | |
| 2. Общая характеристика организации. Комплексный анализ (исследование) состояния информационной безопасности организации | | |
| 3.Должностные обязанности практиканта | | |
| 4. Характеристика деятельности (задач) на производственной практике. | | |
| 5. Практические результаты деятельности студента полученные в ходе практики | | |
| *(вопросы, подлежащие изучению в соответствии с планируемыми результатами обучения,*  *заполняются руководителем практики от МЭИ)* | | |

**По результатам прохождения практики студент оформляет отчет по установленной форме.**

|  |  |  |
| --- | --- | --- |
| Руководитель практики  (от МЭИ) |  | / Артёмов А.С. / |
|  | *(подпись)* | (*Фамилия и инициалы*) |

|  |  |  |
| --- | --- | --- |
| Студент |  | / Скальский Е.М. / |
|  | *(подпись)* | (*Фамилия и инициалы*) |

График прохождения практики

|  |  |  |
| --- | --- | --- |
| Номер  п/п | Перечень работ в соответствии с заданием на практику | Отметка о выполнении работы  (выполнено /не выполнено) |
| 1 | Подготовительный этап: Инструктаж, сбор и систематизация информации по организации прохождения практики (кафедра БИТ, ИнЭИ, НИУ МЭИ) | 15.06-20.06 |
| 2 | Этап прохождения практики: Выполнение индивидуального задания производственной практики. | 21.06-28.06 |
| 3 | Заключительный этап: Разработка и оформление отчета и презентации | 29.06-04.07 |
| 4 | Защита отчета | 04.07-12.07 |

|  |  |  |
| --- | --- | --- |
| Руководитель практики (от МЭИ) |  | / Артёмов А.С. / |
|  | *(подпись )* | (*Фамилия и инициалы*) |

Содержание

[Введение 4](#_Toc138797432)

[Глава 1. Общая характеристика организации 5](#_Toc138797433)

[1.1. Общая информация об организации 5](#_Toc138797434)

[1.2. Активы организации 6](#_Toc138797435)

[1.3. Информационные активы компании 6](#_Toc138797436)

[1.4. Компьютерная и сетевая инфраструктура 6](#_Toc138797437)

[1.5. Программное обеспечение 7](#_Toc138797438)

[1.6. Программные (программно-аппаратные) средства защиты информации 8](#_Toc138797439)

[1.7. Физические средства защиты 9](#_Toc138797440)

[1.8. Комплексный анализ состояния информационной безопасности учебного учреждения 10](#_Toc138797441)

[10. Сбои в системе безопасности: сбои в системе безопасности могут привести к утечке конфиденциальных данных или к несанкционированному доступу к ним. 14](#_Toc138797442)

[Вывод по первой главе 14](#_Toc138797443)

[Глава 2. Результаты выполнения индивидуального задания 15](#_Toc138797444)

[2.1. Должностные обязанности 15](#_Toc138797445)

[2.2. Характеристика деятельности на производственной практике 16](#_Toc138797446)

[2.3. Практические результаты деятельности 16](#_Toc138797447)

[Вывод по второй главе 17](#_Toc138797448)

[Заключение 17](#_Toc138797449)

[Список используемых источников 18](#_Toc138797450)

# **Введение**

**Актуальность** данной практической работы является ввод студента в мир информационной безопасности, уже как не просто студента, а как практически специалиста информационной безопасности. Она является актуальной, так как информационная безопасность развивается с каждым годом, и не собирается терять свою актуальность ближайшее время, поэтому в ней нужны новые специалисты по информационной безопасности.

**Цель практической работы** – это получение практических навыков и умений сотрудника информационной безопасности в области информационной безопасности, освоение профессиональных компетенций.

Для реализации цели используются следующие задачи:

1. Изучить активы и информационные активы учебного заведения;
2. Изучить компьютерную и сетевую инфраструктуру учебного заведения.
3. Изучить программное обеспечение учебного заведения, программные (программно-аппаратные) средства защиты информации;
4. Изучить физические средства защиты информации;
5. Провести комплексный анализ состояния информационной безопасности учебного учреждения.

# **Глава 1. Общая характеристика организации**

* 1. **Общая информация об организации**

Национальный исследовательский университет «МЭИ» — ведущий вуз России в области энергетики, электротехники, радиотехники, электроники и информационных технологий. Адрес Красноказарменная ул., 17, стр. 3, Москва

НИУ «МЭИ» располагает обширной материально-технической базой, включающей в себя 12 институтов, более 100 научно-исследовательских лабораторий, специализированный опытный завод, уникальную учебную ТЭЦ, крупнейшую научно-техническую библиотеку в стране, полигон возобновляемой энергии.

В университете по 25 направлениям подготовки проходят обучение более 20 000 студентов и аспирантов. Высокое качество обучения и научной деятельности обеспечивают.

* 1. **Активы организации**

Сотрудники Учебного заведения – более 1600 преподавателей и учёных, в том числе 184 доктора и 597 кандидатов наук.

Клиенты – в большей степени клиентами учебного заведения МЭИ являются выпускники школ и колледжей желающие получить высшее образование.

Программное обеспечение: БАРС, сайт МЭИ, Прометей, почта МЭИ ОСЭП.

* 1. **Информационные активы компании**

В учебном заведении представлены следующие информационные активы: Лицензия на программное обеспечение, БАРС, сайт МЭИ, Прометей.

Введём степени критичности объектов защиты: 3 – минимальная, 2 – средняя, 1 – высокая. По текущей шкале оценим критичность объектов защиты:

* БАРС 1
* сайт МЭИ 1
* Прометей 3
* МЭИ ОСЭП
  1. **Компьютерная и сетевая инфраструктура**

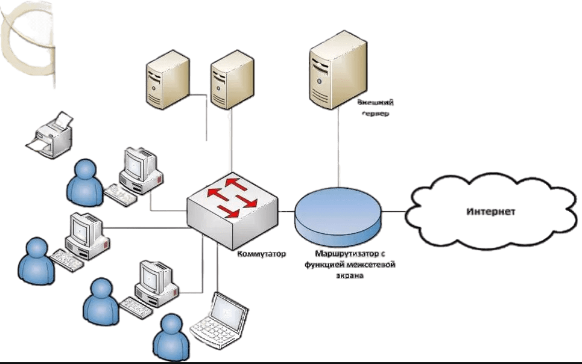


Рис.1 Структурная схема сети предприятия

Средство аутентификации: для входа в систему, требуется выбрать логин и ввести пароль. Компьютеры автоматически подключены к внешнему сетевому хосту, с помощью которого они могут работать с созданными внутри сети сайтами, для работы не на рабочем компьютере учебного заведения, придется долго настраивать подключение, со знанием логина и пароля. Порядок учета и маркировки присутствует.

Степень критичности сетевых устройств: В случае выхода из строя компьютера, в учебном учреждении имеется множество специалистов по работе с компьютера, которые смогу его починить. Также в компании присутствует маршрутизатор и коммутатор, которые обеспечивают построение всей сети учебного заведения. Они являются критичными устройствами.

Учетные записи: в программном обеспечении БАРС есть база данных всех пользователей, в ней можно настраивать права доступа пользователей, добавлять пользователей, удалять пользователей и многие другие функции как для студентов, так и для преподавателей

* 1. **Программное обеспечение**

БАРС - (БАлльно-Рейтинговая Система) – автоматизированная информационная система, являющаяся программной реализацией балльно-рейтинговой системы для студентов НИУ «МЭИ».

МЭИ ОСЭП - В НИУ "МЭИ" для поддержки единой корпоративной почты функционирует подсистема **ОСЭП. ПОЧТА,** которая предоставляет каждому студенту, аспиранту, сотруднику и другим представителям контингента вуза персональный почтовый ящик МЭИ. ОСЭП. ПОЧТА в автоматическом режиме актуализирует корпоративную адресную книгу. Подсистема предоставляет функционал для ведения групповых списков рассылки. Сотрудники, зарегистрированные в корпоративной сети МЭИ, входят в список рассылки расчетных листков. Сотрудники НИУ МЭИ имеют возможность запросить создание списка рассылки, указав круг лиц, которые должны войти в этот список, и ответственного за поддержание списка рассылки в актуальном состоянии

* 1. **Программные (программно-аппаратные) средства защиты информации**

Учебная лаборатория **"Программно-аппаратной защиты информации"**, имеющая 16 автоматизированных рабочих мест, со специальным программным обеспечением, функционирующих на базе операционной системы Windows, и специальное лабораторное оборудование, предназначенное для выполнения лабораторных работ по следующим дисциплинам:

* Технические средства охраны, по которой выполняется две лабораторные работы.
* Программно-аппаратные средства защиты информации, по которой выполняется четырнадцать лабораторных работ.
* Криптографические методы защиты информации, по которой выполняется пять лабораторных работ.
* Администрирование систем и сетей, по которой выполняется четыре лабораторные работы.
* Обеспечение безопасности электронного бизнеса, по которой выполняется две лабораторные работы.
* Защита и обработка конфиденциальных документов, по которой выполняется три лабораторные работы.
  1. **Физические средства защиты**

**Адрес местонахождения:** 111250, Россия, г. Москва, ВН.ТЕР.Г. МУНИЦИПАЛЬНЫЙ ОКРУГ ЛЕФОРТОВО, УЛ КРАСНОКАЗАРМЕННАЯ, Д.14, СТР.1. Так же у МЭИ есть множество корпусов и различных строений, в которых проводятся как обычные мероприятия в виде пар, так и более развлекательные и интеллектуальные занятия.

* **Главный учебный корпус (корпуса: А, Б, В, Г, Д)**
* **Административный корпус (корпуса: Ж, З, И, К, Л)**
* **Корпус Е**
* **Корпус М**
* **Корпус Н**
* **Корпус Р**
* **Корпус C**
* **Корпус Т**
* **Корпус Ф**
* **Корпус X**
* **Дом культуры МЭИ**
* **Научно-техническая библиотека МЭИ**
* **Опытный завод**
* **Стрелково-спортивный тир МЭИ**
* **Стадион "Энергия"**
* **Спортивно-оздоровительный комплекс МЭИ. Бассейн**
* **Санаторий-профилакторий МЭИ**
* **Учебно-экспериментальная теплоэлектроцентраль МЭИ**

Так же имеется 8 общежитий

В каждом перечисленном месте учебное заведение НИУ МЭИ имеет как минимум 1 КПП с турникетом на главный вход в здания, дополнительные входы/входы из зданий учебного учреждения МЭИ, также оснащены охраной с турникетом. которые активно используются для более быстрого доступа в часть здания, которая относительно далеко от главного входа здания Так же по всей территории учебного учреждения находятся камеры видеонаблюдения для большей безопасности сотрудников и студентов. Помещения зданий так же оснащены пожарно-охранной сигнализацией, которая вызывает в случае сигнала службу пожарной охраны

* 1. **Комплексный анализ состояния информационной безопасности учебного учреждения**

Анализ информационной системы учебного учреждения– разработка модели угроз и уязвимостей согласно методике ФСТЭК.

Описание возможных внешних и внутренних нарушителей и их целей приведены

Таблица 1. Возможные виды нарушителей

|  |  |  |
| --- | --- | --- |
| Виды нарушителя | Категория | Возможные цели |
| Отдельные физические лица | Внешний | • Получения материальной выгоды  • Любопытство  • Сбор информации, необходимой для реализации другой угрозы |
| Конкурирующие организации | Внешний | • Получение конкурентного преимущества  • Кража интеллектуальной собственности |
| Лица, обеспечивающие функционирование систем и сетей | Внутренний | • Получение материальной выгоды  • Непреднамеренные действия |
| Авторизованные пользователи систем и сетей | Внутренний | • Получение материальной выгоды  • Непреднамеренные действия  • Умышленные действия в собственных интересах (месть и т.п.) |
| Специалисты IT и ИБ отделов | Внутренний | • Получение материальной выгоды  • Непреднамеренные действия  • Умышленные действия в собственных интересах (месть и т.п.) |
| Бывшие работники | Внешний | • Получение материальной выгоды  • Умышленные действия в собственных интересах (месть и т.п.) |

В случае реализации угроз злоумышленниками, возможны негативные последствия, представленные в таблице 2

Таблица 2. Виды рисков и типовые негативные последствия от реализации угроз безопасности информации

|  |  |  |
| --- | --- | --- |
| № | Виды ущерба | Возможные типовые негативные последствия |
| У1 | Ущерб физическому лицу | финансовый ущерб в результате мошенничества, потери данных или преследования. |
| У2 | Риски юридическому лицу | может понести ущерб в виде потери прибыли, денежных штрафов, расходов на восстановление, унижения доверия клиентов, немощности соблюдать программы или договоры с партнерами. |

**К возможным объектам воздействия относится:**

* АРМ сотрудников организации:
* АРМ директора организации;
* БАРС
* Почта МЭИ ОСЭП
* База данных сотрудников и студентов
* Сайт МЭИ

Классификации уязвимостей информационных систем используются следующие классификационные признаки по ГОСТу Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»:

**Уязвимости ИС по области происхождения уязвимости:**

* уязвимости архитектуры;
* организационные уязвимости.

**Уязвимости ИС по типам недостатков ИС:**

* недостатки, связанные с неправильной настройкой параметров ПО;
* недостатки, приводящие к утечке/раскрытию информации ограниченного доступа;
* недостатки, связанные с управлением полномочиями;
* недостатки, связанные с управлением разрешениями, привилегиями и доступом.

**Уязвимости ИС по месту возникновения:**

* уязвимости в прикладном ПО;
* уязвимости в специальном ПО.

**Угроза безопасности информации**. В модели угроз безопасности информации учебного учреждения рассматриваются перечисленные в разделе угрозы безопасности информации:

1. Несанкционированный доступ к информации: это может быть вызвано хакерами, злоумышленниками, внутренними сотрудниками или студентами, которые могут получить доступ к конфиденциальной информации, такой как личные данные студентов и персонала, финансовые данные и т.д.

2. Вредоносное программное обеспечение: это может быть вызвано вирусами, червями или троянскими программами, которые могут заразить компьютеры и серверы учебного учреждения и привести к потере данных или нарушению работы систем.

3. Физические угрозы: это может быть вызвано пожарами, наводнениями, землетрясениями или другими природными бедствиями, которые могут повредить оборудование и привести к потере данных.

4. Социальная инженерия: это может быть вызвано злоумышленниками, которые могут использовать социальную инженерию для получения доступа к конфиденциальной информации путем обмана сотрудников или студентов.

5. Нарушение политик безопасности: это может быть вызвано неправильным использованием паролей, отсутствием обновлений безопасности или неправильным хранением конфиденциальной информации.

6. Нарушение конфиденциальности: это может быть вызвано утечкой конфиденциальной информации через электронную почту, социальные сети или другие каналы связи.

7. Нарушение целостности данных: это может быть вызвано изменением или удалением данных без разрешения, что может привести к потере важной информации.

8. Нарушение доступности данных: это может быть вызвано отказом в обслуживании, сбоями оборудования или другими техническими проблемами, которые могут привести к недоступности данных для пользователей.

**Способы реализации угроз безопасности информации:**

1. Физический доступ к компьютеру или серверу: злоумышленник может получить доступ к компьютеру или серверу, на котором хранятся конфиденциальные данные, и скопировать или изменить их.

2. Вирусы и вредоносное ПО: злоумышленники могут использовать вирусы и другое вредоносное ПО для заражения компьютеров и кражи конфиденциальных данных.

3. Социальная инженерия: злоумышленники могут использовать социальную инженерию, чтобы обмануть пользователей и получить доступ к конфиденциальным данным.

4. Несанкционированный доступ к сети: злоумышленники могут получить несанкционированный доступ к сети, на которой хранятся конфиденциальные данные, и скопировать или изменить их.

5. Недостаточная защита паролей: недостаточно сложные пароли могут быть легко угаданы или подобраны злоумышленниками.

6. Недостаточная защита сетевых устройств: некоторые сетевые устройства могут быть уязвимыми для атак, если они не обновляются регулярно или не защищены соответствующими мерами.

7. Недостаточная защита приложений: некоторые приложения могут быть уязвимыми для атак, если они не обновляются регулярно или не защищены соответствующими мерами.

8. Недостаточная защита сетевых коммуникаций: некоторые сетевые коммуникации могут быть уязвимыми для атак, если они не защищены соответствующими мерами шифрования и аутентификации.

9. Физические атаки на оборудование: злоумышленники могут физически атаковать оборудование, на котором хранятся конфиденциальные данные, чтобы получить доступ к ним.

# 10. Сбои в системе безопасности: сбои в системе безопасности могут привести к утечке конфиденциальных данных или к несанкционированному доступу к ним.

# **Вывод по первой главе**

В итоге проанализировав активы учебного учреждения, программное обеспечение, компьютерную и сетевую инфраструктуру и все средства защиты организации, была разработана модель угроз данного учебного учреждения. В модели угроз были описаны возможные виды как внутренних, так и внешних нарушителей, на основе которых можно сказать, что самые вероятные нарушители – это авторизованные пользователи систем и сетей, обладающие базовыми возможностями и системные администраторы (обладающие базовыми повышенными возможностями), а также просто бывшие сотрудники. Также были определены актуальные угрозы безопасности информации, способы реализации, описанных угроз и уязвимости ИС. Кроме того, были проанализированы виды рисков и типовые негативные последствия от реализации угроз безопасности информации и возможные объекты воздействия.

# **Глава 2. Результаты выполнения индивидуального задания**

## 2.1. Должностные обязанности

Одной из моих обязанностей в МЭИ, было уничтожение старых рефератов, срок годности КИ которых истек, для этого использовался шредер уничтожающий бумагу и др. возможные виды носители информации без возможности восстановления (Флешки, диски). Так же моей обязанностью было тестирование функциональности системы БАРС на новом ПО, для ее работоспособности. В ходе выполнения было нужно находить ошибки в системе, и заносить их сайт, где эти ошибки уже рассмотрит другой человек и решит проблему. Для полного выполнения задания было выдана инструкция для тестирования и выданы права начальника курса ИнЭИ, для большего ознакомления с системой БАРС, не только по правам студента. Так для тестирования БАРС на не рабочем компьютере МЭИ, нужно было подключиться к VPN МЭИ через vpngui.

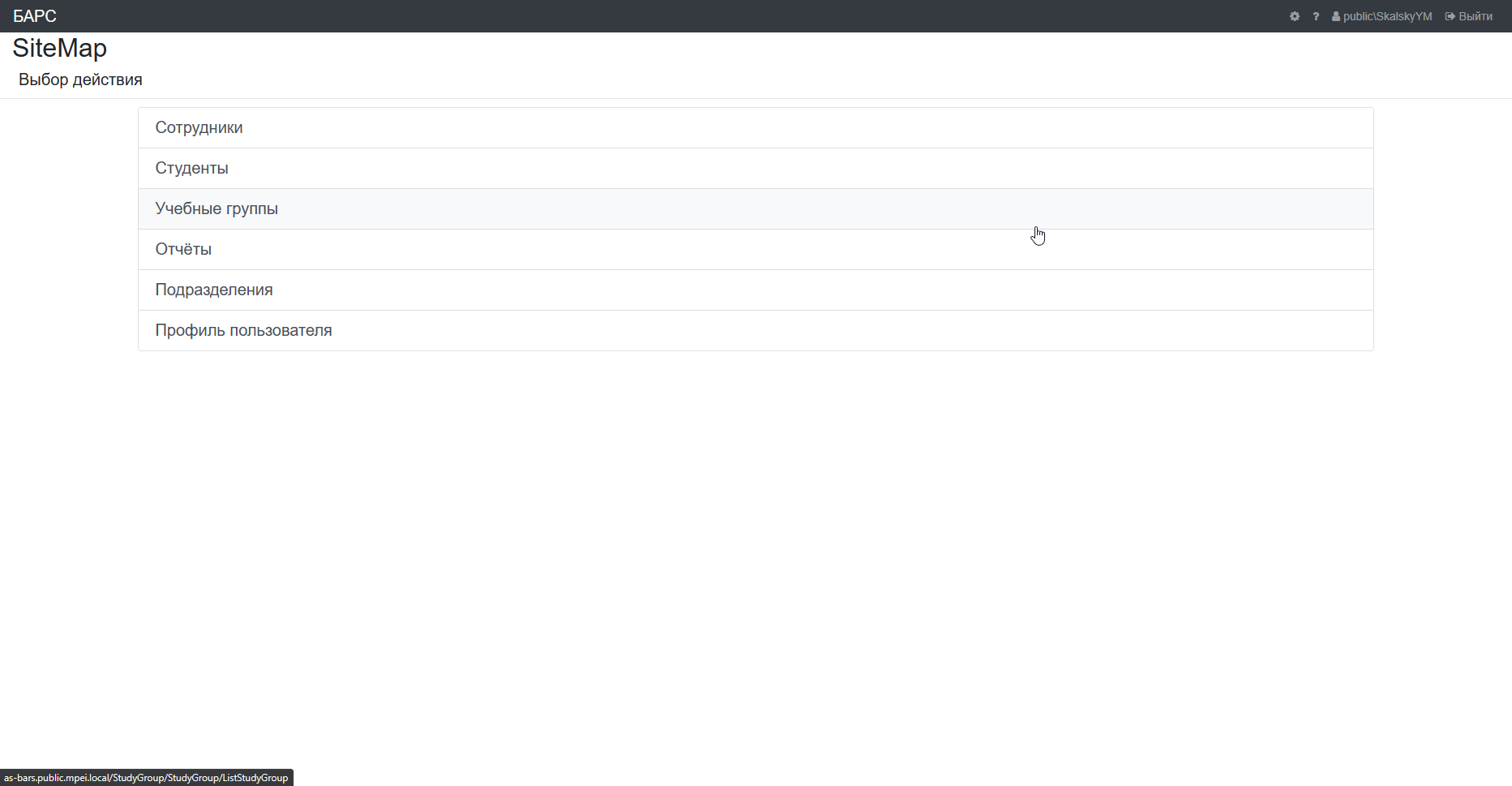


Рис 2. Расширенный функционал начальника курса в БАРС

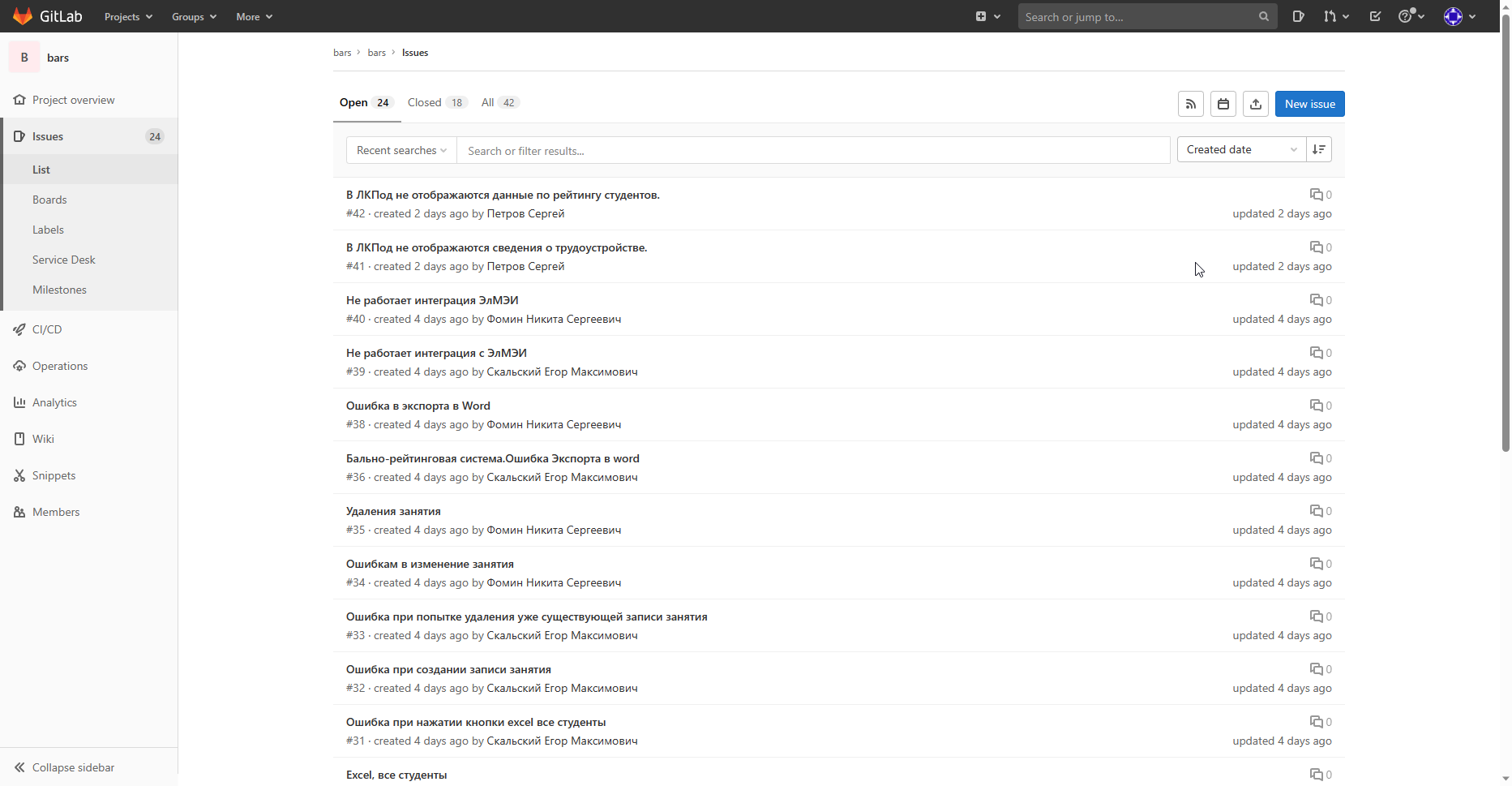


Рис 3. Занесенные ошибки всех тестировщиков

## 2.2. Характеристика деятельности на производственной практике

В ходе прохождения практики мною были получены следующие навыки:

1. Был изучен более открытый интерфейс студента в роли старосты
2. Был изучен полный функционал сотрудников МЭИ
3. Научился создавать пары, КМ, листы групп и др. функционал преподавателя МЭИ
4. Научился исправлять оценки, пропуски, и др. функционал преподавателей в БАРС в роли начальника курса.
5. Научился уничтожать КИ

## 2.3. Практические результаты деятельности

Результатами деятельности является то, что во время уничтожения КИ в виде дипломов студентов, никто не сможет их забрать себе, а также узнать кто был песцом данной работы, с его ПДн. А благодаря моему тестированию БАРСа, мы смогли обнаружить множество ошибок как, из-за которых не работала сама система БАРС, на новом ПО, так и исключаем возможности злоумышленников попасть на сайт и получить некую КИ официальных пользователей данной платформы и не только.

# **Вывод по второй главе**

Таким образом, в ходе выполнения индивидуальных заданий во время производственной практики, мною была изучена схема уничтожения без возможности восстановления бумажных документов.

Так же благодаря мне, были найдены некоторые ошибки БАРС из-за которых было невозможно работать в этой платформе до тех пор, пока не пофиксят ошибки. И получил практические навыки по работе в системе БАРС с продвинутыми возможностями

# **Заключение**

Таким образом, можно сделать следующие выводы

1. Были изучены активы и информационные активы учебного учреждения;
2. Мною была нарисована компьютерная и сетевая инфраструктура учебного заведения;
3. Было изучено программное обеспечение, программные средства защиты информации учебного учреждения;
4. Были изучены физические средства защиты компании;
5. Мною была разработана методика оценки угроз безопасности информации.
6. Мною была изучена более подробная система БАРС
7. Мною были выявлены различные ошибки и баги в системе БАРС
8. Мною было изучено методика уничтожения документов без возмоности востановления

# **Список используемых источников**

1. Банк угроз и уязвимостей ФСТЭК. URL: <https://bdu.fstec.ru/> (дата обращения: 17.06.2023);
2. БАРС МЭИ. URL. <http://as-bars.public.mpei.local/Auth/Menu> (Дата обращения 17.06.2023);
3. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» URL: <https://docs.cntd.ru/document/1200123702> (дата обращения: 18.06.2023);
4. Методика оценки угроз безопасности информации. ФСТЭК России, 2021 год. URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g> (дата обращение 18.06.2023);
5. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ Общий доступ: сетевой журнал.

<URL:https://www.consultant.ru/document/cons_doc_LAW_61801/> (дата обращения: 19.06.2023).

1. GitLab. URL: [Issues · bars / bars · GitLab (cbias.ru)](https://git.cbias.ru/bars/bars/-/issues?scope=all&utf8=%E2%9C%93&state=opened) (Дата обращения: 21.06.2023)