Министерство транспорта Российской Федерации

Федеральное агентство железнодорожного транспорта

ФГБОУ ВО “ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ

УНИВЕРСТИТЕТ ПУТЕЙ И СООБЩЕНИЯ”

Кафедра: ”Информационные технологии

и системы”

ОТЧЕТ

по производственной практике

(научно-исследовательской работе)

Студент гр. СО251КОБ Козеко М.В.

Руководитель

доцент, к.т.н. Гурвиц Г.А.

Хабаровск

2021

СОДЕРЖАНИЕ

[ЗАДАНИЕ 3](#_Toc69073045)

[ХАРАКТЕРИСТИКА 5](#_Toc69073046)

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 6](#_Toc69073047)

[ВВЕДЕНИЕ 7](#_Toc69073048)

[ПОНЯТИЕ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 8](#_Toc69073049)

[ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННЫХ СИСТЕМ 10](#_Toc69073050)

[ПРОГРАММА ДЛЯ ПАРСИНГА УГРОЗ 13](#_Toc69073051)

[ФРАГМЕНТ КОДА ПРОГРАММЫ 16](#_Toc69073052)

[ДНЕВНИК ПРАКТИКИ 18](#_Toc69073053)

[ЗАКЛЮЧЕНИЕ 19](#_Toc69073054)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 20](#_Toc69073055)

# ЗАДАНИЕ

на производственную практику (научно-исследовательскую работу) для студента специальности 10.05.03 «Информационная безопасность автоматизированных систем»

**Цель практики**: Выбор темы и подбор материала для ВКР

**Содержание практики:**

* Определение понятий информации и информационной безопасности;
* Ознакомление с основными документами, используемыми при работе в области информационной безопасности;
* Анализ алгоритма по выбору мер и средств защиты информации в информационных системах;
* Выбор темы ВКР и изучение соответствующего теоретического материала;
* Оформление отчета.

Примерное содержание отчета по производственной практике (НИР):

1. Определение понятий информации и информационной безопасности;
2. Основные документы, используемые при работе в области информационной безопасности;
3. Основные характеристики информационных систем;
4. Реализация программы для парсинга информационных угроз в локальную базу данных с банка данных угроз ФСТЭК;
5. Дневник практики;
6. Список литературы.

|  |  |  |
| --- | --- | --- |
| Задание выдано студенту | Козеко М.В.\_\_\_\_\_\_  (Фамилия И.О.) | Группы СО251КОБ |
| Руководитель практики | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | Г.А.Гурвиц |



# ХАРАКТЕРИСТИКА

Выдана студенту 5-го курса Дальневосточного государственного университета путей сообщения института «Управления, автоматизации и телекоммуникаций» по направлению *подготовки «Информационная безопасность автоматизированных систем» Козеко Михаилу Вячеславовичу,* проходившему производственную практику (НИР) с 09.03.2021 по 06.04.2021.

Во время прохождения практики (НИР) изучал нормативно-правовую базу в сфере информационной безопасности, проанализировал алгоритм по выбору мер и средств защиты информации в информационных системах;

Все рекомендуемые нотации, наставления принимал и выполнял на должном уровне, относился к работе добросовестно. Студент показал себя инициативным и способным действовать самостоятельно, продемонстрировал высокий уровень исполнительной дисциплины. За время практики Козеко М.В. освоил все необходимые для работы теоретические и практические навыки.

Козеко М.В. овладел следующими компетенциями:

* способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
* способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
* способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
* способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

Достигнут 3 уровень (знать, уметь, владеть) оценки показателей владения вышеуказанными компетенциями.

Замечаний по прохождению практики нет.

В целом работу на практике можно оценить самой высокой оценкой.

Руководитель практики,

к.т.н., доцент Гурвиц Г.А.

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Я, Козеко Михаил Вячеславович, студент 5 курса специальности «Информационная безопасность автоматизированных систем» Дальневосточного государственного университета путей сообщения группы СО51КОБ с 09.03.21 по 06.04.21, проходил производственную практику в ПАО Сбербанк (ЦА), блок “Технологии”, Департамент ИТ блока “Розничный бизнес”, Управление ИТ “Сберегательные продукты”.

На время прохождения практики основной задачей являлся сбор теоретической информации для написания дипломной работы.

При прохождении практики:

* Определил понятия информации и информационной безопасности;
* Ознакомился с основными документами, используемыми при работе в области информационной безопасности;
* Провел анализ основных характеристик информационных систем;
* Написал программу для парсинга информационных угроз в локальную базу данных с банка данных угроз ФСТЭК

# ВВЕДЕНИЕ

Информационная безопасность предназначена для обеспечения конфиденциальности и целостности информации, недопущение несанкционированных действий с ней, в частности, ее использования, раскрытия, искажения, изменения, исследования и уничтожения. Положения информационной безопасности одинаковы для всех форм хранения информации: физических, цифровых или любых других. С появлением компьютеризированных информационных систем безопасность данных вышла на первый план.

Использование систем информационной безопасности ставит перед собой конкретные задачи по сохранению ключевых характеристик информации и обеспечивает:

* конфиденциальность данных – доступ есть только у лиц, имеющих на это полномочия;
* доступность информационных систем с находящимися в них данными конкретным пользователям, у которых есть право доступа к таким сведениям;
* целостность данных предполагает блокировку несанкционированного изменения информации;
* подлинность – полнота и общая точность информации;

# ПОНЯТИЕ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Главная цель систем информационной безопасности – гарантия защиты данных от внешних и внутренних угроз.

Для обеспечения в информационной системе полной конфиденциальности применяются четыре метода, актуальных для любого формата информации:

* ограничение или полное закрытие доступа к информации;
* шифрование;
* дробление на части и разрозненное хранение;
* скрытие самого факта существования информации.

Для определения правильной стратегии информационной защиты необходимо определить, что угрожает безопасности данных. Угрозы информационной безопасности – вероятные события и действия, которые в перспективе способны привести к утечке или потере данных, несанкционированному доступу к ним. Это, в свою очередь, приведет к моральному или материальному ущербу.

Основным регулятором в области защиты информации является Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

ФСТЭК России осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

* обеспечения безопасности информации в ключевых системах информационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;
* противодействия иностранным техническим разведкам на территории Российской Федерации;
* технической защиты информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом;
* осуществления экспортного контроля.

**Противодействие иностранным техническим разведкам (ПД ИТР)** – деятельность, направленная на исключение или затруднение получения иностранными техническими разведкам разведывательной информации об объектах защиты.

**Техническая защита информации (ТЗИ)** – деятельность, направленная на обеспечение некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических и средств.

**Обеспечение безопасности информации в ключевых системах информационной инфраструктуры (ОБИ в КСИИ)** – деятельность, направленная на исключение или затруднение реализации в отношении управляющих информационных систем деструктивных воздействий, в результате которых может сложиться чрезвычайная ситуация.

**Экспортный контроль (ЭК)** – деятельность, направленная на исключение при осуществлении внешнеэкономической деятельности незаконного распространения товаров, информации, работ и услуг, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники либо при подготовке и свершении террористических актов.

**Техническая защита информация (ТЗИ),** обеспечение безопасности информации в ключевых системах информационной инфраструктуры (ОБИ в КСИИ) заключаются в проведении мероприятий по обеспечению неизменности свойств безопасности информации, таких как конфиденциальность, целостность, доступность. Необходимо исключить утечку информации, ее уничтожение (модификацию) и блокирование. При этом достигается цель по нейтрализации актуальных угроз реализующихся по техническим каналам, за счет несанкционированного доступа и иных специальных воздействий.

**Информация**– сведения (сообщения, данные) независимо от формы их предоставления.

**Документированная информация** – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

**Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

# ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННЫХ СИСТЕМ

На основе анализа информационных систем и основных нормативно-правовых документов России в области информационной безопасности была составлена таблица основных характеристик информационных систем:

|  |  |
| --- | --- |
| Параметры ИС | Классификация параметра ИС |
| Структура объектов защиты | Локальная ИС |
| Распределенная ИС |
| Архитектура ИС | Клиент-серверная ИС |
| Файл-серверная ИС |
| Наличие (отсутствие) взаимосвязей ИС с иными ИС | Взаимодействует |
| Не взаимодействует |
| Категории обрабатываемых ПД | Специальные |
| Биометрические |
| Общедоступные |
| Иные категории |
| Объем обрабатываемых ПД | Менее 100 000 субъектов |
| Более 100 000 субъектов |
| Категория субъектов ПД | Субъекты персональных данных, не являющиеся сотрудниками |
| Субъекты персональных данных, являющиеся сотрудниками (обработка персональных данных работников; субъектов, с которыми ваша организация связана трудовыми отношениями) |
| Тип актуальных угроз | угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн; |
| угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн; |
| угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн. |
| Требуемый **уровень защищенности** ПД | 1 УЗ |
| 2 УЗ |
| 3 УЗ |
| 4 УЗ |
| **Класс защищенности** ИС (При использовании в ГИС) | 1 КЗ |
| 2 КЗ |
| 3 КЗ |
| Режим обработки информации | многопользовательский |
| однопользовательский |
| Режим разграничения прав доступа пользователей | с разграничением прав |
| без разграничения прав |
| Режим разделения функций по управлению информационной системой | с разделением |
| без разделения |
| Сегментирование информационной системы | с сегментированием |
| без сегментирования |
| По размещению технических средств | в пределах одной контролируемой зоны |
| в пределах нескольких контролируемых зоны |
| Наличие (отсутствие) взаимосвязей ИС (подключений) к сетям связи общего пользования | подключена к сетям общего пользования |
| не подключена к сетям общего пользования |
| Программные и технические средства обработки ПДн в ИС | Перечень программных и технических средств |
| Состав технических средств обработки ПДн в ИС | Перечень состава технических средств |
| Топология сети | Представляет из себя схематичное изображение элементов системы |
| Перечень актуальных угроз | Формируется на основе документа "модель угроз" |
| Тип актуальных угроз | 1 тип |
| 2 тип |
| 3 тип |
| Существующие средства защиты | Перечень средств |
| Существующие меры защиты | Перечень мер |
| Вид/тип нарушителя | Внешние субъекты/внешний |
| Пользователи ИС/внутренний |
| Потенциал нарушителя | Базовый (низкий) |
| Базовый повышенный (средний) |
| Высокий |

# ПРОГРАММА ДЛЯ ПАРСИНГА УГРОЗ

В ходе выполнения практики была написана программа, которая позволяет получить список угроз безопасности информации с банка данных угроз ФСТЭК и добавить эти угрозы в локальную базу данных для дальнейшей работы с данными угрозами.

Интерфейс программы:

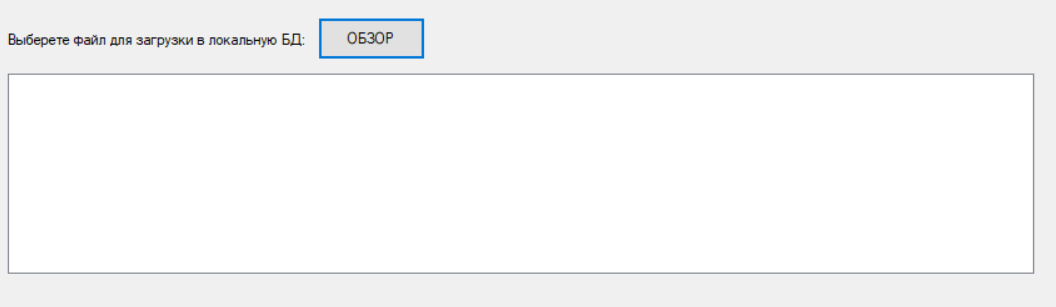


Рисунок 1 Интерфейс программы

Исходными данными для работы программы является файл xlsx который требуется скачать с сайта банка данных угроз ФСТЭК:

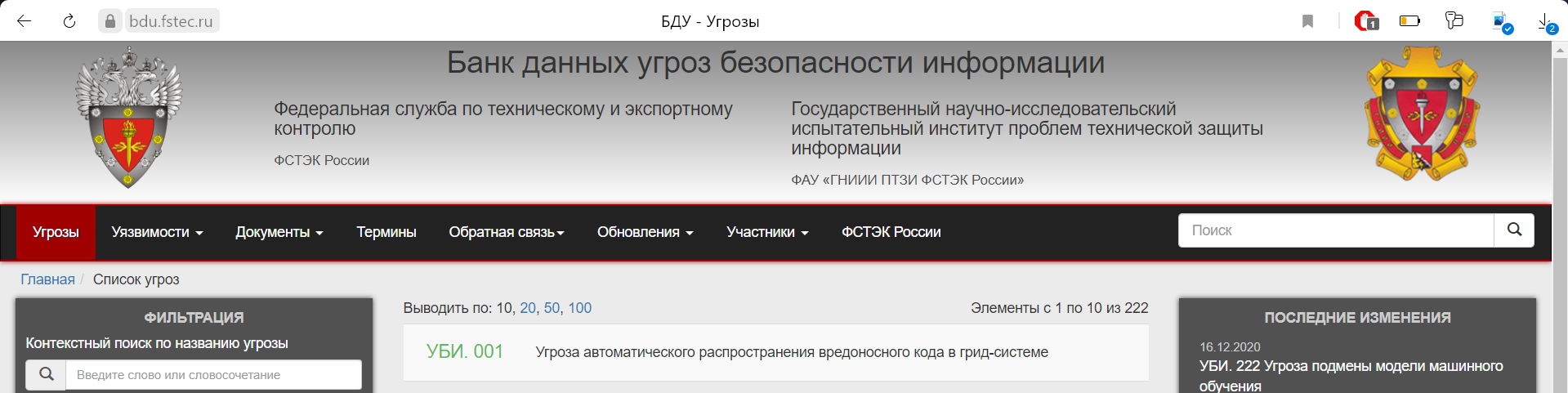


Рисунок 2 Сайт банка данных угроз ФСТЭК

Кнопка “Скачать сведения об угрозах”:

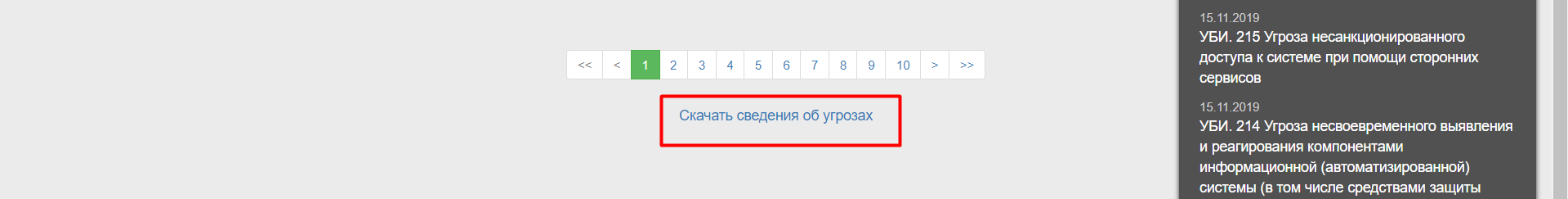


Рисунок 3 Кнопка "Скачать сведения об угрозах"

Данный файл содержит в себе сведения об актуальных угрозах информационной безопасности:

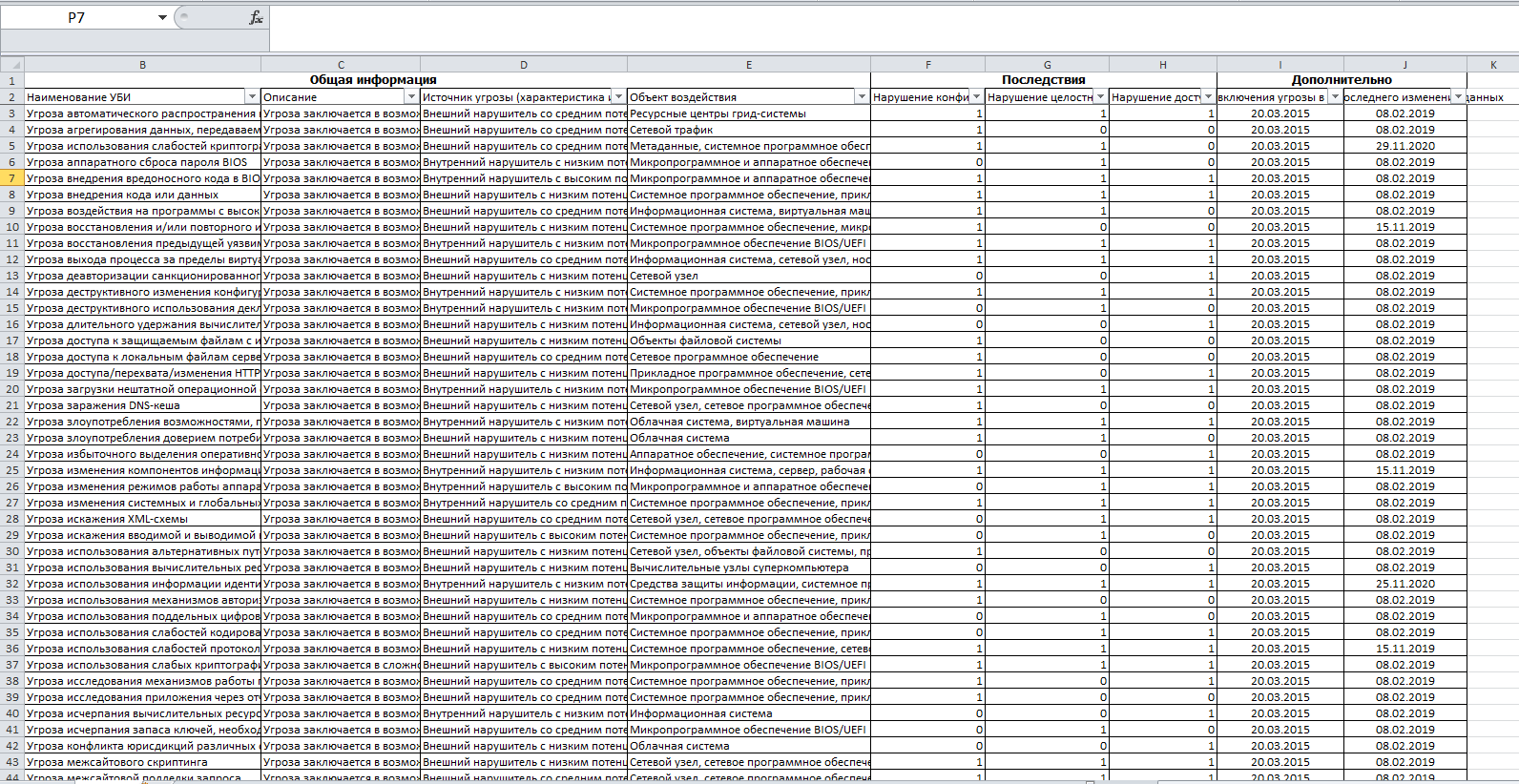


Рисунок 4 Содержимое файла xlsx

Для загрузки файла в программу требуется нажать клавишу “Обзор” и выбрать файл xlsx:



Рисунок 5 Этап загрузки файла в программу

После успешной загрузки данных в БД программа показывает список загруженных в БД строк и столбцов

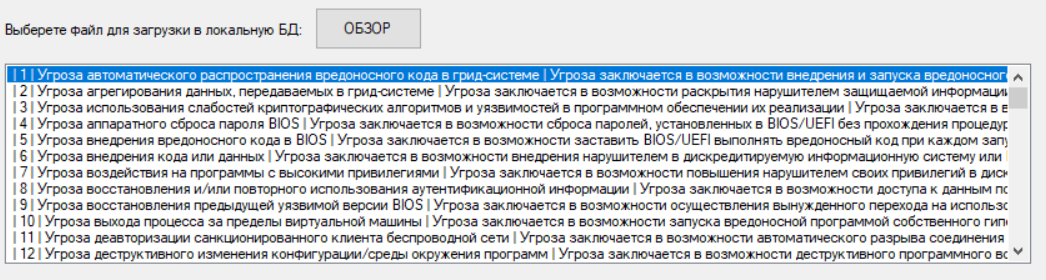


Рисунок 6 Список загруженных данных

Данные в БД успешно загружены:

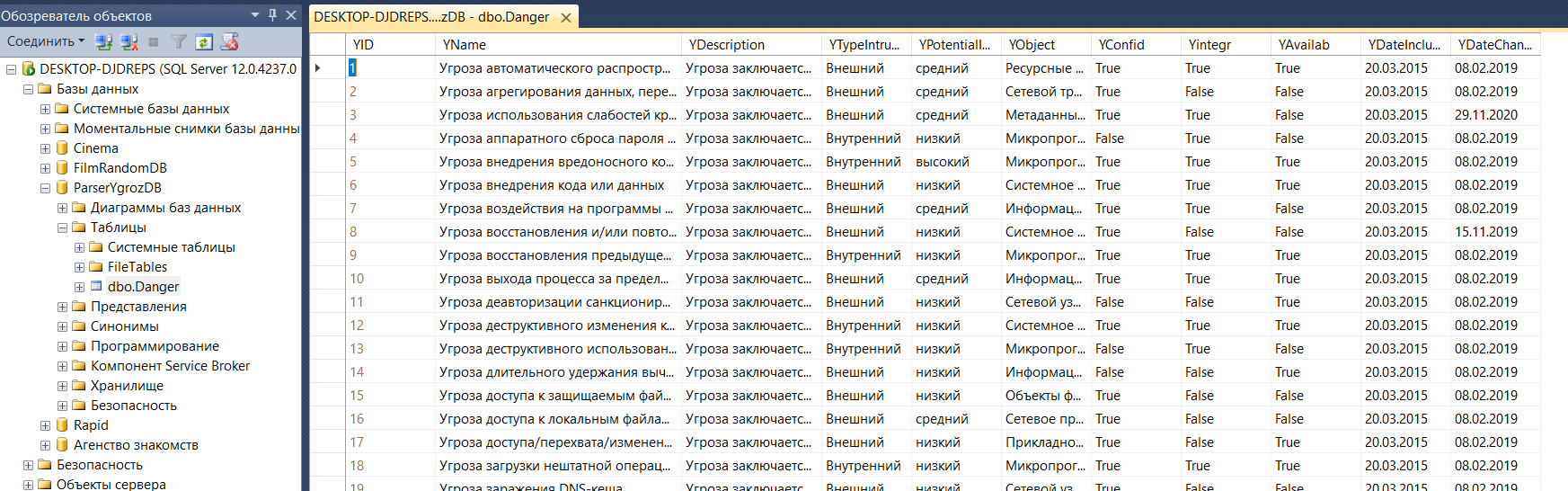


Рисунок 7 Список загруженных данных в локальной БД

Данная программа предназначена для того, чтобы в дальнейшем быстро актуализировать информацию об актуальных угрозах ФСТЭК при работе с информационными системами, в частности в дипломном проекте.

В качестве темы для ВКР была выбрана тема: “Разработка программного комплекса по выбору мер защиты информации для их реализации в информационных системах”.

# ФРАГМЕНТ КОДА ПРОГРАММЫ

private string[,] ImportEx() //Функция импорта файла excel в массив mass

{

//Выбор файла

OpenFileDialog ofd = new OpenFileDialog();

//Расширение по умолчанию

ofd.DefaultExt = "\*.xls;\*xlsx";

// Задаем заголовок диалогового окна

ofd.Title = "Выберите файл excel";

if (!(ofd.ShowDialog() == DialogResult.OK)) // если файл excel не выбран -> Выход

{

MessageBox.Show("Ошибка в выборе файла");

string[,] mass = new string[0, 0];

return mass;

}

else

{

Excel.Application ObjWorkExcel = new Excel.Application();

Excel.Workbook ObjWorkBook = ObjWorkExcel.Workbooks.Open(ofd.FileName);

Excel.Worksheet ObjWorkSheet = (Excel.Worksheet)ObjWorkBook.Sheets[1]; //получить 1-й лист

var lastCell = ObjWorkSheet.Cells.SpecialCells(Excel.XlCellType.xlCellTypeLastCell);//последнюю ячейку

int lastColumn = (int)lastCell.Column;// размеры базы (столбцы и строки)

int lastRow = (int)lastCell.Row;

//Перенос данных в массив mass

string[,] mass = new string[lastRow-2, lastColumn]; // число строк на 2 меньше чем в excel, потому что первые 2 строки в excel - это заголовки

for (int j = 0; j < lastColumn; j++) //по всем столбцам

for (int i = 0; i < lastRow; i++) //по всем строкам

{

if (i == lastRow - 2 || i == lastRow -1)

{

continue;

}

mass[i, j] = ObjWorkSheet.Cells[i + 3, j + 1].Text.ToString(); //Считывание данных(пропуск первых двух строк с заголовками в excel)

}

ObjWorkBook.Close(false, Type.Missing, Type.Missing); //закрыть не сохраняя

ObjWorkExcel.Quit(); // выйти из Excel

GC.Collect(); // убрать за собой

return mass;

}

}

//Разбиение массива mass по столбцам

private List<string> MakeCollum(string[,] mass, int collum)

{

List<string> list = new List<string>();

for (int i = 0; i < mass.GetLength(0);i++)

{

list.Add(mass[i, collum]);

}

return list;

}

private void AddNewDanger(string[,] mass)

{

ParserYgrozDBContext context = new ParserYgrozDBContext();

for (int i = 0; i < mass.GetLength(0); i++)

{

Danger danger = new Danger();

for (int j = 1; j < mass.GetLength(1); j++)

{

if (j == 1)

danger.YName = mass[i, j];

if (j == 2)

danger.YDescription = mass[i, j];

if (j == 3)

{

if (mass[i, j].Contains("Внешний"))

danger.YTypeIntruder = "Внешний";

else

danger.YTypeIntruder = "Внутренний";

if (mass[i, j].Contains("высоким"))

danger.YPotentialIntruder = "высокий";

else if (mass[i, j].Contains("средним"))

danger.YPotentialIntruder = "средний";

else

danger.YPotentialIntruder = "низкий";

}

if (j == 4)

danger.YObject = mass[i, j];

if (j == 5)

if (mass[i, j] == "1")

danger.YConfid = true;

else

danger.YConfid = false;

if (j == 6)

if (mass[i, j] == "1")

danger.Yintegr = true;

else

danger.Yintegr = false;

if (j == 7)

if (mass[i, j] == "1")

danger.YAvailab = true;

else

danger.YAvailab = false;

if (j == 8)

danger.YDateInclude = mass[i, j];

if (j == 9)

danger.YDateChange = mass[i, j];

context.Danger.Add(danger);

}

}

context.SaveChanges();

}

}

# ДНЕВНИК ПРАКТИКИ

Сроки практики: 09.03.2021-06.04.2021

|  |  |
| --- | --- |
| Период | Этап |
| 09.03.2021-  13.03.2021 | Определений понятий информации и информационной безопасности |
| 13.03.2021-15.03.2021 | Ознакомление с основными документами, используемыми при работе в области информационной безопасности |
| 15.03.2021-17.03.2021 | Анализ основных характеристик информационных систем |
| 17.03.2021-20.03.2021 | Настройка среды программирования “Visual Studio” |
| 20.03.2021-22.03.2021 | Подготовка базы данных на “MS SQL Server” |
| 22.03.2021-  04.04.201 | Разработка программы |
| 04.04.2021-06.04.2021 | Подготовка отчета |



Руководитель практики Гурвиц Г.А.

# ЗАКЛЮЧЕНИЕ

В результате прохождения практики были получены профессиональные умения и опыт по изучению нормативно-правовых документов в области информационной безопасности. В результате ознакомления с рядом нормативно-правовых актов, государственных стандартов и методических рекомендаций были приобретены теоретические навыки, необходимые при разработке информационной системы. Конечным результатом данной практики является программа по парсингу угроз в локальную базу данных с банка данных угроз ФСТЭК.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон от от 27.07.2006 № 149-ФЗ, ред. от 18.03.2019 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/, свободный. – Загл. с экрана.
2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: приказ ФСТЭК РФ от 11.02.2013 №17 – Режим доступа: http://fstec.ru/component/attachments/download/567, свободный. – Загл. с экрана.
3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 № 1119 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_137356/, свободный. – Загл. с экрана.
4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ ФСТЭК РФ от 18.02.2013 №21 – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, свободный. – Загл. с экрана.
5. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006, свободный. – Загл. с экрана.
6. О персональных данных [Электронный ресурс]: федер. закон от от 27.07.2006 № 152-ФЗ, ред. от 31.12.2017 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61801, свободный. – Загл. с экрана.