МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Брянский государственный технический университет»
Кафедра «Системы информационной безопасности»

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

по направлению подготовки 10.04.01– «Информационная безопасность»
на тему: Разработка методики определения актуальных угроз безопасности информации в информационных системах

Магистрант группы: О-18-ИБ-ози-М
Клищенко М.П.
Руководитель работы: к.т.н., доц.
Голембиовская О.М.

Брянск 2021

Актуальность

По данным статистического анализа зарубежных компаний лабораторией «Kaspersky ICS CERT», 2019 год подтвердил глобальный характер киберугроз. Зафиксированы кибератаки на следующие объекты:

- **электроэнергетическая компания на западе США;**
- **компания ASCO Industries;**
- **японский производитель оптического оборудования HOYA;**
- **бельгийский горно-металлургический комбинат Nyrstar;**
- **норвежская металлургическая компания Norsk Hydro;**
- **компания «Одинцовский Водоканал» (РФ).**

Данная статистика показывает, что вопрос определения угроз информационной безопасности требует более тщательного изучения, а также поиска и разработки дополнительных решений.

Объект, предмет и научная новизна исследования

Объект исследования – процесс оценки актуальных угроз в информационных системах.

Предмет исследования – методики определения актуальных угроз информационной безопасности.

Научная новизна - разработана методика определения актуальных угроз, с применением аддитивной свертки в части определения вероятности реализации угроз (групп угроз), а также разработан подход к оценке степени ущерба.

Цель и задачи исследования

Цель – сокращение временных затрат на выявление актуальных угроз безопасности ИС, а также повышение качественного уровня оценки данных угроз.

Задачи:

- Изучить стандарты и нормативно-правовые документы, относящиеся к методикам и средствам определения актуальных угроз.
- Определить возможность реализации различных видов угроз безопасности информации, при помощи оценки уровня защищённости от угроз ИБ с применением аддитивной свертки.
- Разработать подход к определению степени возможного ущерба.
- Определить актуальные угрозы безопасности информации в информационных системах.
- Разработать организационные меры для повышения уровня защиты информации в информационных системах.
- Разработать автоматизированную систему определения актуальных угроз безопасности информации.

Анализ нормативно-правовой базы и международных стандартов

№, п/п	Наименование нормативно-правового документа	Статьи, затрагивающие вопросы исследования	Применимость в рамках исследования
1	Доктрина информационной безопасности РФ	Документ целиком	Определены основные цели, задачи, принципы и направления обеспечения информационной безопасности
2	Федеральный закон «Об информации, информационных технологиях и защите информации»	Статья 2, 8-11, 16, 17	Определены базовые понятия, касающиеся информационной безопасности, порядок распространения информации, доступа и ограничения доступа к информации, цели и меры для защиты информации и ответственность за правонарушения
3.	ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности»	Документ целиком	Определяет структуру обеспечения приватности

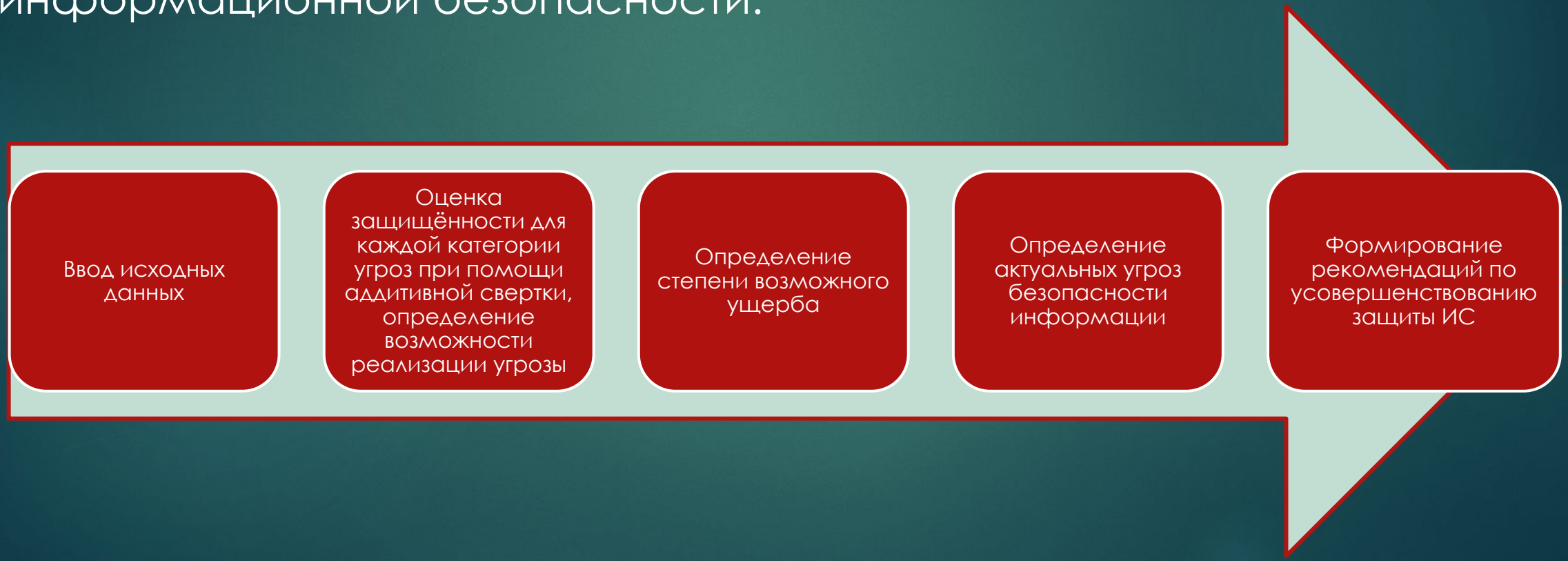
Нормативно-правовые документы в области информационной безопасности

№, п/п	Наименование стандарта	Статьи, затрагивающие вопросы исследования	Применимость в рамках исследования
1	BS 7799 Code of Practice for Information Security Management	Первая часть	Формирование цели информационной защиты данных
2	ISO 17799 Information technology - Security techniques - Code of practice for information security management	Документ целиком	Определяет требования, используемые при создании устойчивой структуры безопасности, особое внимание необходимо уделять комплексному подходу, направленному на управление безопасности.
3	ISO/IEC 27001 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования»	Документ целиком	Содержит описания лучших мировых практик в области управления информационной безопасностью. Устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы

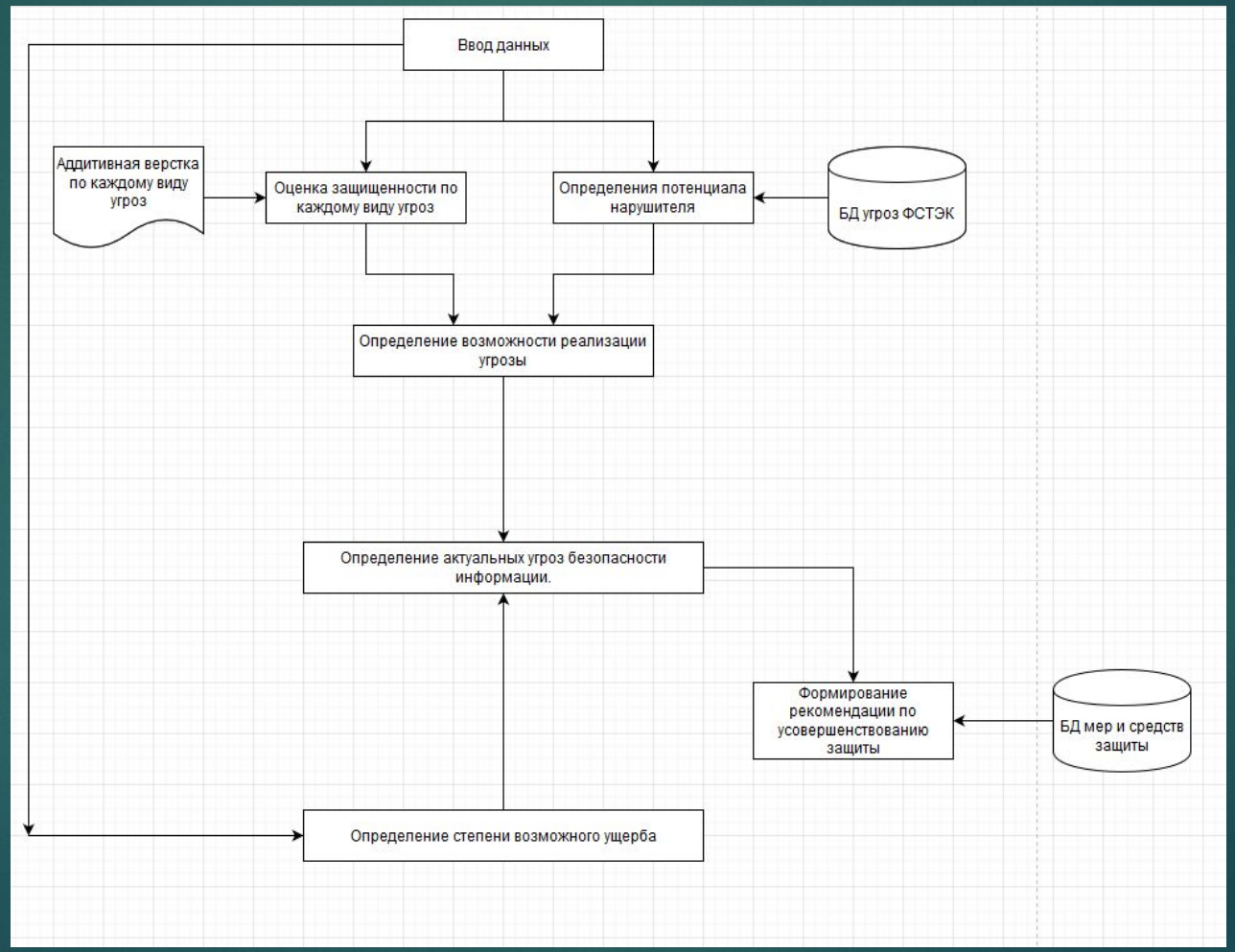
Международные стандарты в области информационной безопасности

Методика определения актуальных угроз информационной безопасности

Этапы работы методики определения актуальных угроз информационной безопасности:



Структурно-функциональная схема работы методики



Аддитивная свертка для оценки защищённости на примере угроз, связанных с неблагоприятными событиями природного, техногенного и социального характера

№	Частный показатель	Оценка частного показателя (Ch)	Важность (a)
1	**Как часто проводится резервное копирование защищаемой информации?**		0,43
	-не проводится	0	
	-1 раз в год	0,3	
	-1 раз в 6 месяцев	0,5	
	-1 раз в месяц	0,8	
	-2-3 раза в месяц	1	
2	**Используются ли устройства бесперебойного питания?**		0,16
	-не используются	0	
	-используются аккумуляторы	0,5	
	-используются генераторы бензиновые/дизельные	1	
3	**Как регламентирована и реализуется политика пожарной безопасности?**		0,13
	-не регламентирована, не реализована	0	
	-регламентирована документально, не реализована техническими и организационными мерами	0,2	
	-регламентирована документально, реализована техническими и организационными мерами	1	
4	**Как часто проводятся проверки программных и аппаратных средств защиты информации?**		0,07
	-не проводятся	0	
	-проводятся перед приездом проверяющей комиссии	0,1	
	-проводятся 1 раз в год	0,2	
	-проводятся 1 раз в 6 месяцев	0,4	
	-проводятся 1 раз в месяц	1	
5	**Используются ли водостойкие и огнестойкие сейфы для хранения носителей конфиденциальной информации**		0,21
	-сейфы не используются вообще	0	
	-используются обычные сейфы	0,2	
	-используются водостойкие и огнестойкие сейфы	1	

Аддитивная свертка для оценки защищённости, на примере угроз, связанных с несоответствием требованиям надзорных и регулирующих органов действующему законодательству

№	Частный показатель	Оценка частного показателя	Важность (a)
1	**Соответствует ли организация требованиям приказа ФСТЭК №21?**		0,15
	-не соответствует	0	
	-соответствует частично	0,2	
	-соответствует полностью	1	
2	**Соответствует ли организация требованиям Постановления Правительства РФ № 1119?**		0,25
	-не соответствует	0	
	-соответствует частично	0,2	
	-соответствует полностью	1	
3	**Соответствует ли организация требованиям ФЗ №152?**		0,30
	-не соответствует	0	
	-соответствует частично	0,2	
	-соответствует полностью	1	
4	**Соответствует ли организация требованиям Постановления Правительства РФ № 687?**		0,2
	-не соответствует	0	
	-соответствует частично	0,2	
	-соответствует полностью	1	
5	**Соответствует ли организация требованиям РД АС?**		0,1
	-не соответствует	0	
	-соответствует частично	0,2	
	-соответствует полностью	1	

Аддитивная свертка для оценки защищённости по каждому виду угроз

Оценка группового показателя (GP) производится посредством аддитивной свертки коэффициента важности (a) и числовой оценки параметра (Ch), по формуле:

$$GP=a1Ch1+a2Ch2 +…+a7Chn.$$

В соответствии с Методикой определения актуальных угроз безопасности при их обработке в информационных системах, оценка возможности реализации угрозы производится по шкале от 0 до 1, а именно:

- 0–0,3 — уровень защищенности низкий, реализация угрозы высокая. В отношении появившихся дополнительных угроз безопасности, меры для защиты информации не могут быть приняты оперативно.

- 0,3–0,6 — уровень защищенности средний, реализация угрозы. В отношении появившихся дополнительных угроз безопасности, меры для защиты информации могут быть приняты оперативно («за часы»).

- 0,6–1 — уровень защищенности высокая, реализация угрозы низкая. В отношении появившихся дополнительных угроз безопасности, меры для защиты информации могут быть приняты с высокой оперативностью («за минуты»).

Определение степени возможного ущерба

Виды ущербов:

- Экономический
- Социальный
- Политический
- Репутационный
- Ущерб субъекту персональных данных
- Технологический ущерб

Общая степень возможного ущерба при реализации угрозы является высокой, если хотя бы для одного из видов ущерба определена высокая степень.

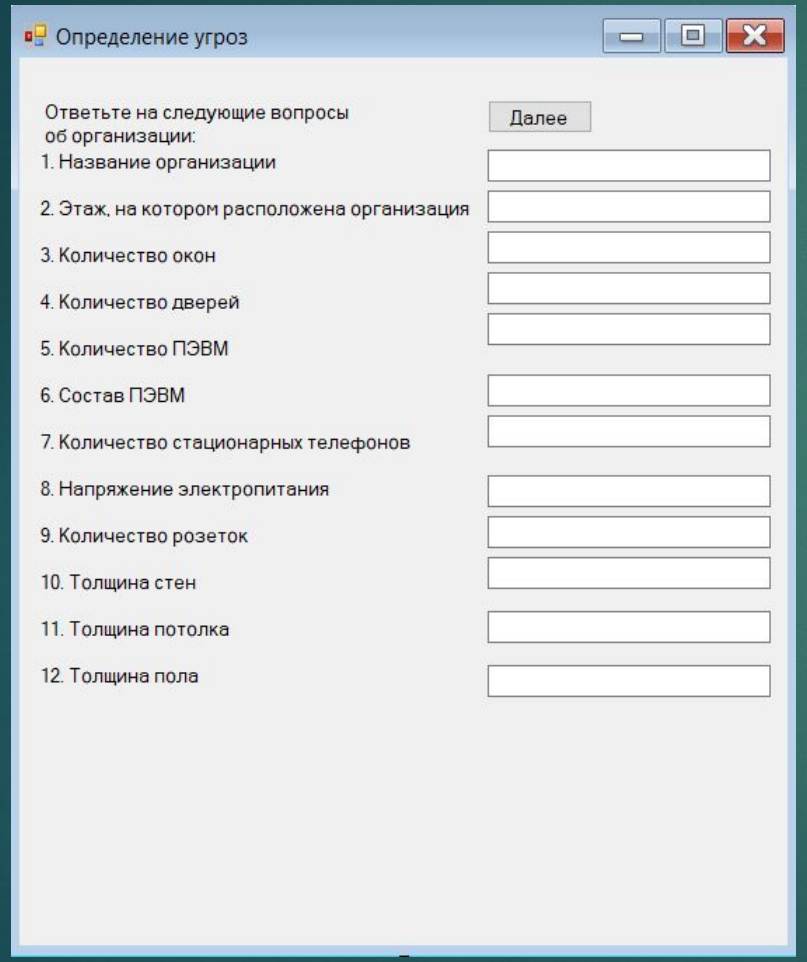
Общая степень возможного ущерба при реализации угрозы является средней, если хотя бы для одного из видов ущерба определена средняя степень и нет ни одного, для которого определена высокая степень.

Общая степень возможного ущерба при реализации угрозы является низкой, если для всех видов ущерба определены низкие степени.

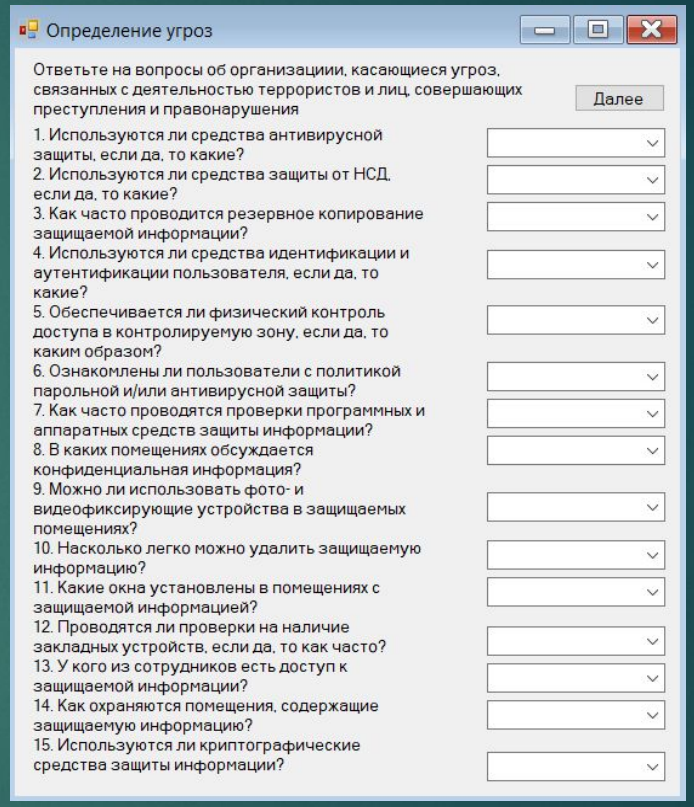
Вопросы для определение уровня возможного ущерба(на примере экономического)

	Ущерб низкий	Ущерб средний	Ущерб высокий
Экономический ущерб			
Отвечает ли система за денежные переводы? Если да, то какова максимальная сумма перевода через систему?			
-не отвечает (ущерб низкий)	+		
- более 75% МРОТ (ущерб высокий)			+
-менее 75% МРОТ (ущерб средний)		+	
Что происходит с денежными средствами в случае расторжения контракта заказчиком?			
-все средства возвращаются к заказчику (ущерб высокий)			+
-часть средств остается в системе (ущерб средний)		+	
Как часто в системе происходят ситуации хищения денежных средств? Если да, то как часто?			
-не происходят (ущерб низкий)	+		
-происходят реже 1 раза в год (ущерб средний)		+	
-происходят чаще 1 раза в год (ущерб высокий)			+
Как часто проводятся проверки работоспособности системы?			
-не проводятся (ущерб высокий)			+
-1 раз в полгода и реже (ущерб средний)		+	
-чаще 1 раза в полгода (ущерб низкий)	+		
Сколько времени требуется для того, чтобы восстановить работоспособность системы после ее поломки или возникновения ошибок в системе?			
-более 1 рабочего дня (ущерб высокий)			+
-1 рабочий день (ущерб средний)		+	
-менее 1 рабочего дня (ущерб низкий)	+		
Какой процент клиентов переходит к конкурентам?			
-не переходят (ущерб низкий)	+		
-до 5% (ущерб средний)		+	
-более 5% (ущерб высокий)			+

Автоматизированная система определения актуальных угроз безопасности информации

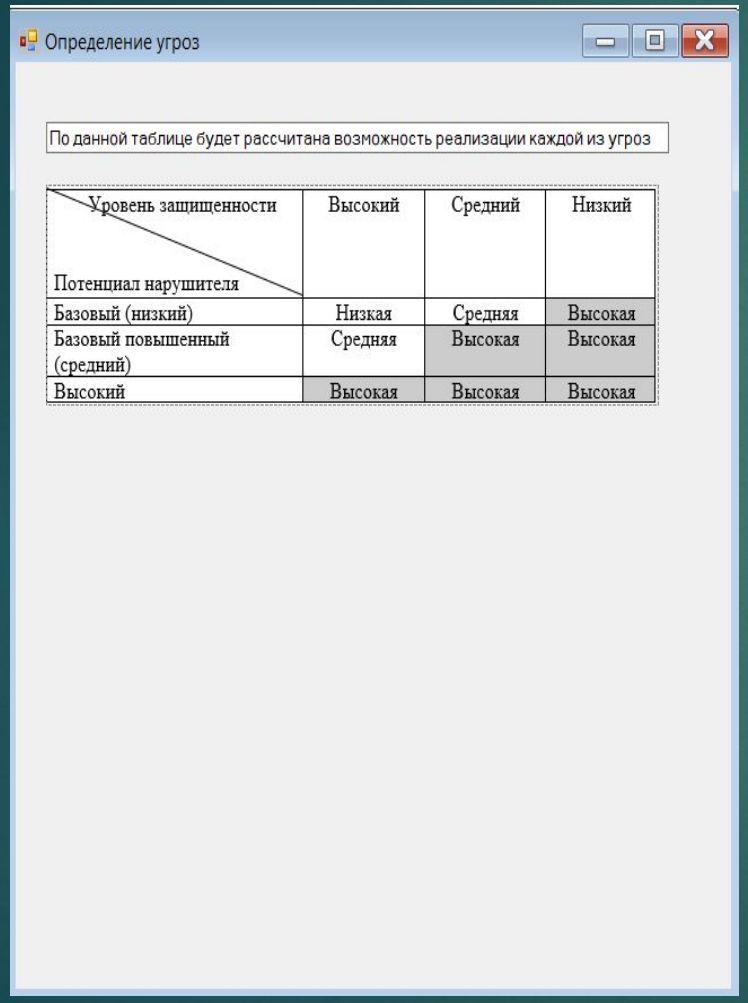


Ввод данных

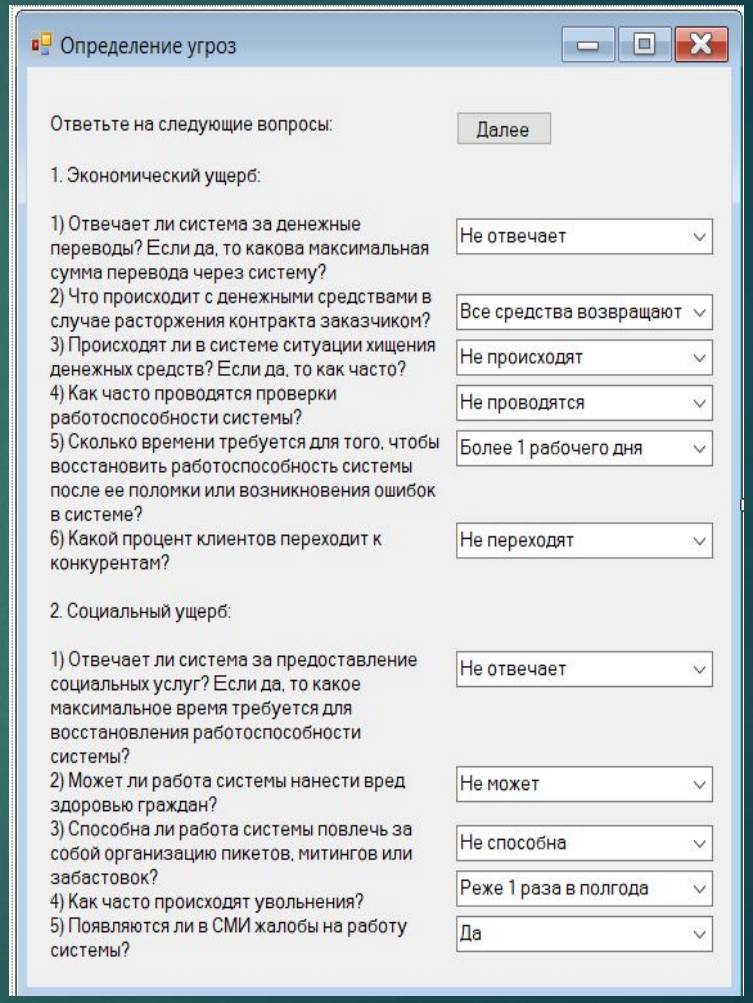


Вопросы для создания свертки для угроз, связанных с деятельностью террористов и лиц, совершающих преступления и правонарушения

Автоматизированная система определения актуальных угроз безопасности информации

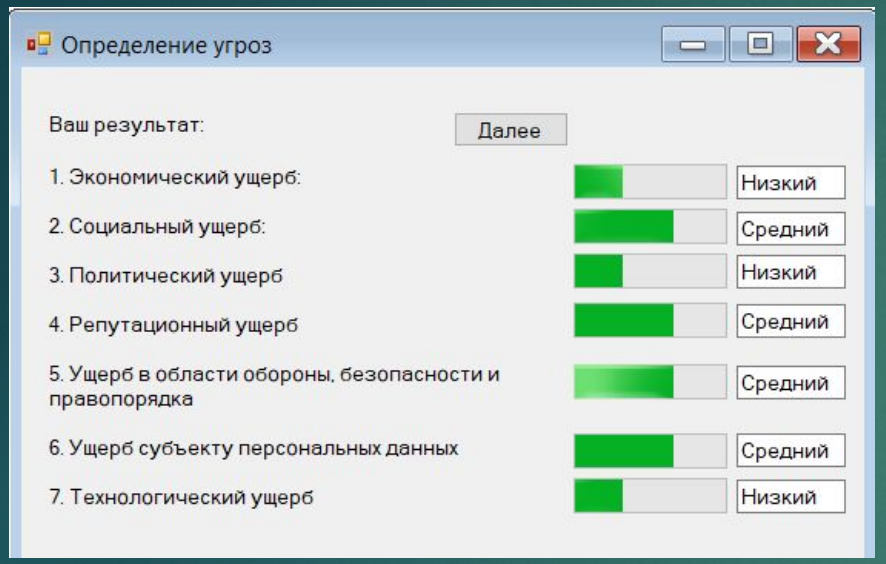


Определение возможности реализации угрозы

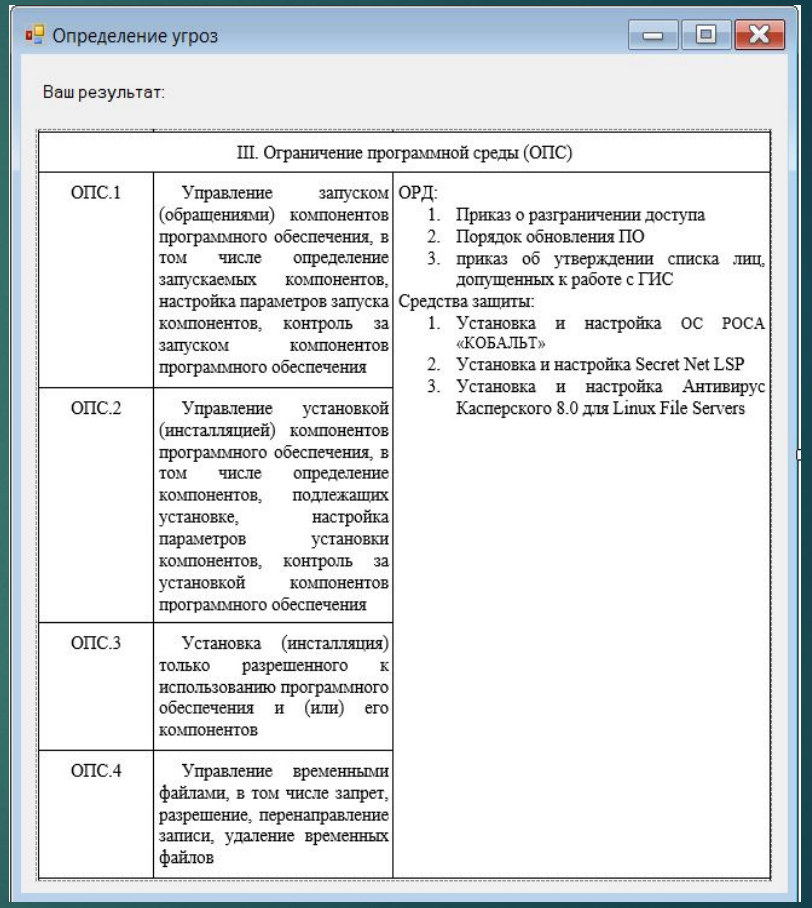


Вопросы для подсчета возможного ущерба

Автоматизированная система определения актуальных угроз безопасности информации



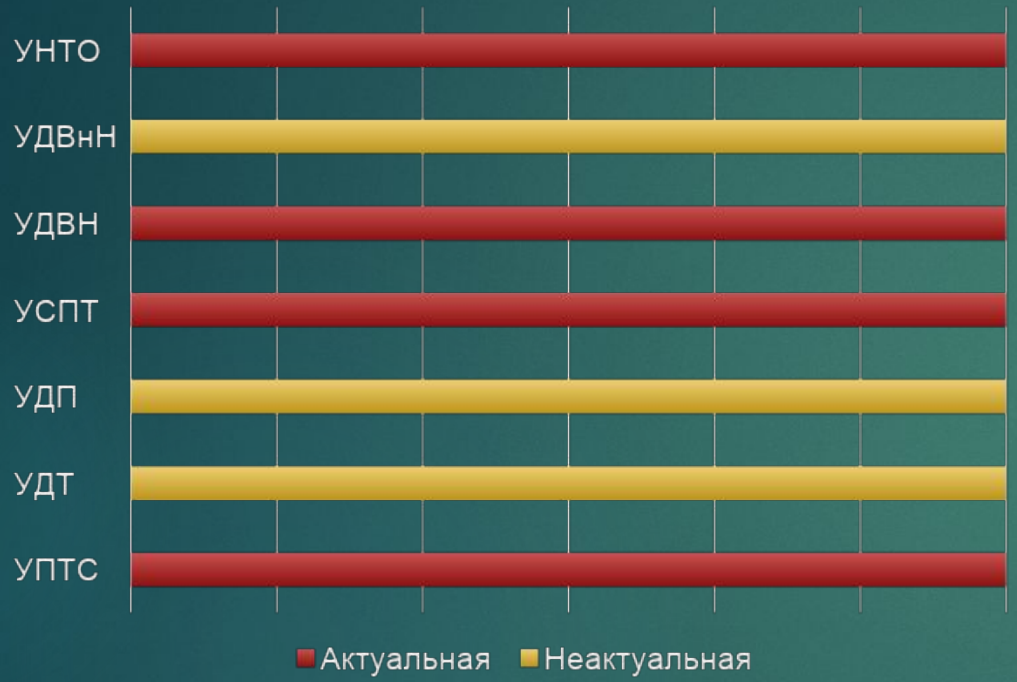
Результаты подсчета степени ущерба по разным видам



III. Ограничение программной среды (ОПС)		
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	ОРД: 1. Приказ о разграничении доступа 2. Порядок обновления ПО 3. приказ об утверждении списка лиц, допущенных к работе с ГИС Средства защиты: 1. Установка и настройка ОС РОСА «КОБАЛЬТ» 2. Установка и настройка Secret Net LSP 3. Установка и настройка Антивирус Касперского 8.0 для Linux File Servers
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	

Рекомендуемые меры защиты информации

Апробация методики на объекте ООО «Бумажный дом»



Актуальные угрозы до апробации методики

Актуальные угрозы после апробации методики

Число актуальных угроз на предприятии снизилось на 43%, что свидетельствует о действенности разработанной системы.

Результаты работы

1. Изучены стандарты и нормативно-правовые документы, относящиеся к методикам и средствам определения актуальных угроз.
2. Составлена методика определения возможности реализации различных видов угроз безопасности информации, при помощи оценки уровня защищённости от угроз ИБ с применением аддитивной свертки.
3. Разработан подход к определению степени возможного ущерба.
4. Определены актуальные угрозы безопасности информации в информационных системах при помощи настоящей методики.
5. Разработана база данных организационных и программах средств защиты возможных к выбору для повышения уровня защиты информационной системы.
6. Разработана автоматизированная система определения актуальных угроз безопасности информации

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Брянский государственный технический университет»
Кафедра «Системы информационной безопасности»

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

по направлению подготовки 10.04.01– «Информационная безопасность»
на тему: Разработка методики определения актуальных угроз безопасности информации в информационных системах

Магистрант группы: О-18-ИБ-ози-М
Клищенко М.П.
Руководитель работы: к.т.н., доц.
Голембиовская О.М.

Брянск 2021