



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Брянский государственный технический университет**

**Факультет информационных технологий**

**Кафедра «Системы информационной безопасности»**

**МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ**

**по направлению подготовки 10.04.01– «Информационная безопасность»  
на тему: Разработка методики определения степени возможного ущерба  
и алгоритма определения уровня защищённости государственных  
информационных систем**

Магистрант группы: О-18-ИБ-ози-М

Клищенко Р.А.

Руководитель работы:

к.т.н., доц., Голембиовская О.М.

Брянск 2021

# АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ



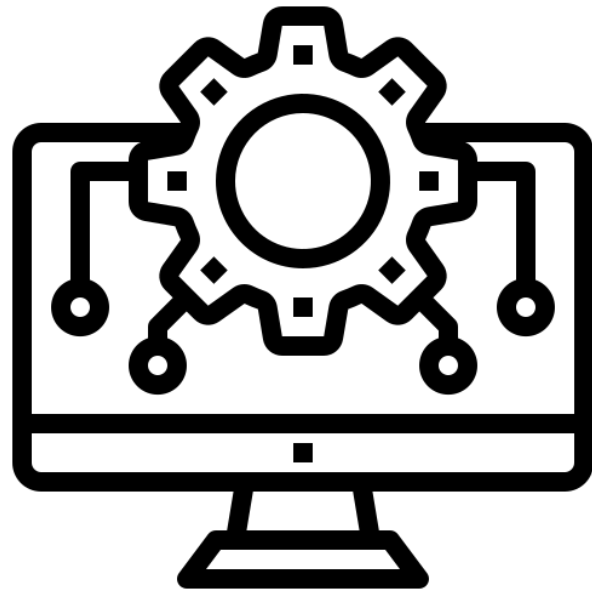
Согласно статистическим данным, в 2019 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое 20 преступление, сообщается на сайте Генеральной прокуратуры Российской Федерации.

# НАУЧНАЯ НОВИЗНА

3

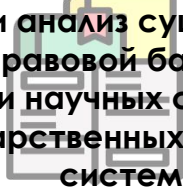
Разработана методика определения степени возможного ущерба, отличающаяся оценкой затрат от негативных последствий, которые могут наступить в случае нарушения свойств информационной безопасности.

Разработан алгоритм определения уровня защищенности государственных информационных систем на основании анализа имеющихся мер защиты информации, посредством применения методики аддитивной свертки



# ЦЕЛЬ И ЗАДАЧИ РАБОТЫ

**Целью работы** является повышение уровня защищённости государственных информационных систем.



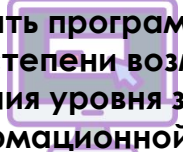
Провести анализ существующей нормативно-правовой базы, методических документов и научных статей в области защиты государственных информационных систем.



Разработать методику определения степени возможного ущерба.



Разработать алгоритм определения уровня защищённости государственных информационных систем.



Разработать программный продукт определения степени возможного ущерба и определения уровня защищённости информационной системы.

# АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В ПРЕДМЕТНОЙ ОБЛАСТИ

№, п/п	Наименование нормативно-правового акта	Статьи, затрагивающие вопросы исследования	Применимость в рамках исследования
1	Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года	п. 1 ст. 13 п. 1 ст. 14	Определение понятия «государственная информационная система». Цель создания ГИС.
2	Приказ ФСТЭК России № 17 от 11 февраля 2013 года	документ целиком	Определение класса защищенности ГИС. Определение базового набора мер защиты информации для установленного класса защищенности ГИС. Определение мероприятий, проводимых оператором ГИС, по обеспечению защиты информации в ходе эксплуатации аттестованной ГИС.
3	Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации ПКЗ-2005, утвержденным Приказом ФСБ России от 09.02.2005г. №66	документ целиком	Порядок разработки СКЗИ. Порядок производства СКЗИ. Порядок эксплуатации СКЗИ.
4	Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»	документ целиком	Определение порядка организации. Обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
5	Методический документ «Меры защиты информации в государственных информационных системах» Утвержден ФСТЭК 11 февраля 2014 года	документ целиком	Набор организационных и технических мер защиты информации в ГИС и правила их реализации

# МЕТОДИКА ОПРЕДЕЛЕНИЯ СТЕПЕНИ ВОЗМОЖНОГО УЩЕРБА

Для оценки степени ущерба ( $\mathcal{E}_y$ ) предполагается следующий подход, отличающаяся оценкой затрат от негативных последствий:

$$\mathcal{E}_y = \mathcal{Ш}_з + \mathcal{O}_y + \mathcal{З}_в + \mathcal{З}_п, \text{ где:}$$

$\mathcal{Ш}_з$  – общая сумма по возможным штрафам от нарушения требований законодательства;

$\mathcal{O}_y$  – оплата сумм по компенсации морального вреда, сформированных в результате решений суда по вопросам разглашения конфиденциальных данных;

$\mathcal{З}_в$  – затраты на восстановление оборудования, в случае его уничтожения/повреждения;

$\mathcal{З}_п$  – затраты, связанные с выплатами (пени/штрафы) от простоя системы.

# МЕТОДИКА ОПРЕДЕЛЕНИЯ СТЕПЕНИ ВОЗМОЖНОГО УЩЕРБА

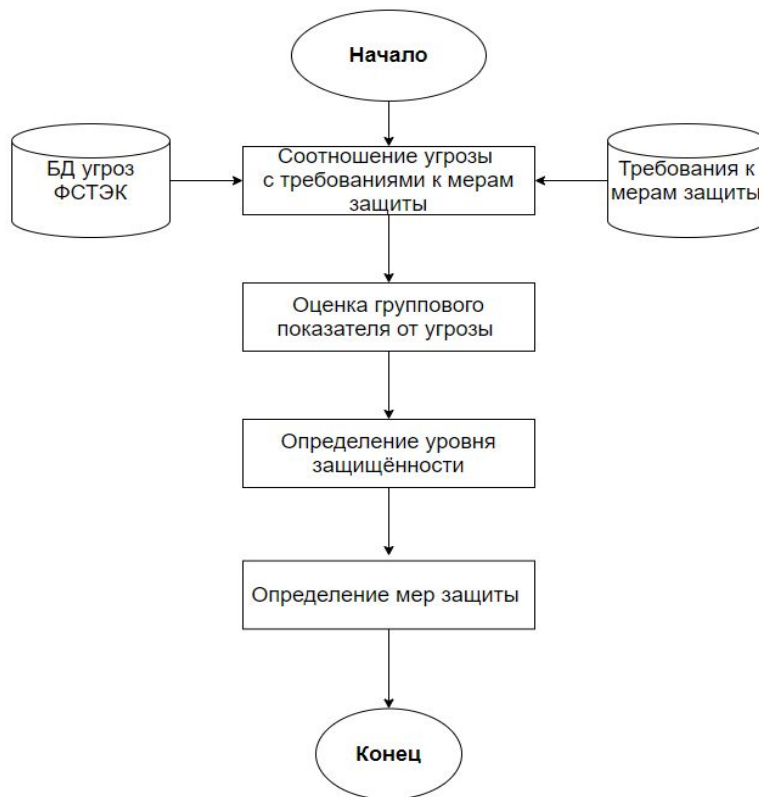
После проведённых расчётов можно сформулировать следующий переход к пояснению негативных последствий:

**Существенные негативные последствия** – ведут к выплате штрафов, компенсаций, иным затратам, составляющим от 50 до 100 % чистого дохода организации (**высокая степень ущерба**).

**Умеренные негативные последствия** – ведут к выплате штрафов, компенсаций, иным затратам, составляющим от 10 до 50 % чистого дохода организации (**средняя степень ущерба**).

**Незначительные негативные последствия** - ведут к выплате штрафов, компенсаций, иным затратам, составляющим до 10 % чистого дохода организации (низкая степень ущерба).

# АЛГОРИТМ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ГИС





# КЛАССИФИКАЦИЯ УГРОЗ ПО ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
<b>1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) (СООТВЕТСТВУЮЩИЕ УГРОЗЫ) <u>3,8,11,30,74,86,98,125,152</u></b>				
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа			

# ОЦЕНКА ГРУППОВОГО ПОКАЗАТЕЛЯ ОТ КАЖДОЙ ГРУППЫ УГРОЗ

Для оценки уровня защищённости предлагается создание аддитивной свертки для каждой группы угроз.

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

$$GP = a_1Ch_1 + a_2Ch_2 + \dots + a_nCh_n.$$

# ОЦЕНКА ГРУППОВОГО ПОКАЗАТЕЛЯ(УРОВНЯ ЗАЩИЩЕННОСТИ) ОТ УГРОЗ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ АЛЬТЕРНАТИВНЫХ ПУТЕЙ ДОСТУПА К РЕСУРСАМ (ПРИМЕР)

11

Обозначение частного показателя	Частный показатель	Оценка частного показателя (Ch)	Важность (a)
28.1	Какие средства по контролю полномочий доступа используются?		0,11
	Не используются	0	
	Используются средства, не имеющие сертификата	0,1	
	DeviceLock 8 DLP Suite	0,3	
	Средство анализа защищенности RedCheck	0,6	
	Ревизор-2 XP	0,9	
28.2	Какие средства защиты от несанкционированного доступа используются?		0,3
	Не используются	0	
	Используются средства, не имеющие сертификата	0,1	
	Персональный идентификатор ШИПКА	0,3	
	СЗИ Dallas Lock 8.0	0,6	
	Электронный замок Соболь 4.2	0,9	
28.3	Какие средства обнаружения вторжений используются?		0,09
	Не используются	0	
	Используются средства, не имеющие сертификата	0,1	
	Средство защиты информации «Континент WAF»	0,3	
	Межсетевой экран и система обнаружения вторжений «Рубикон»	0,6	
	Система обнаружения вторжений ViPNet IDS HS	0,9	
28.4	Какие средства аутентификации/идентификации используются?		0,21
	Не используются	0	
	Используются средства, не имеющие сертификата	0,1	
	Программное обеспечение EMIAS.Kerberos	0,3	
	Модуль доверенной загрузки Numa Arce	0,6	
	Электронный замок Соболь 4.2	0,9	
28.5	Как реализована система видеонаблюдения?		0,29
	Не реализована	0	
	Только снаружи объекта	0,3	
	Только внутри объекта	0,5	
	Снаружи и внутри объекта	0,8	

# ОЦЕНКА ГРУПОВОГО ПОКАЗАТЕЛЯ ОТ КАЖДОЙ ГРУППЫ УГРОЗ

Для формализации процесса определения качественных и количественных значений уровня защищенности представим следующие диапазоны значений:

- ❑ **0 – 0,29 – уровень защищенности низкий**, реализация угрозы высокая, необходимо незамедлительное применение мер защиты, а именно разработка организационных мер и установка средств защиты в соответствии с полученными ответами на вопросы анкеты, которые имели значение от 0 до 0,1, а также теми мерами, которые не выполнены оператором при оценке соответствия Приказу №17 ФСТЭК;
- ❑ **0,3 – 0,59 – уровень защищенности средний**, реализации угрозы средняя, необходимо применение мер защиты, а именно разработка организационных мер и установка средств защиты в соответствии с полученными ответами на вопросы анкеты, которые имели значение от 0 до 0,1, а также теми мерами, которые не выполнены оператором при оценке соответствия Приказу №17 ФСТЭК;
- ❑ **0,6 – 1 – уровень защищенности высокий**, реализации угрозы низкая, незамедлительное применение мер защит не требуется.

# ДЕМОНСТРАЦИЯ РАБОТЫ АС

13

Определение степени возможного ущерба

Оценка уровня защищённости

Начать

Начальное окно работы программы

Параметры определения степени ущерба

Расчет возможных штрафов в связи с нарушением законодательства

Расчет возможных затрат на оплату судебных исков

Затраты на восстановление оборудования, в случае его уничтожения/повреждения

Затраты, связанные с выплатами (пени/штрафы) от простоя системы

Параметры для определения степени возможного ущерба

Результаты определения степени ущерба

Высокая степень возможного ущерба

Начать заново

Вернуться в начало

Результаты определения степени возможного ущерба

# ДЕМОНСТРАЦИЯ РАБОТЫ АС

14

Угроза воздействия на программы с высокими привилегиями
<b>Аппаратно-программные модули доверенной загрузки</b> <input type="checkbox"/> Не используется <input type="checkbox"/> «ЩИТ ЭЦП» <input checked="" type="checkbox"/> «Соболь»
<b>Защита аутентификации и идентификации</b> <input type="checkbox"/> Отсутствует <input checked="" type="checkbox"/> Парольная защита <input type="checkbox"/> Биометрическая защита
<b>Подключение к сети Интернет:</b> <input type="checkbox"/> Присутствует на всех ПК <input type="checkbox"/> Отсутствует <input checked="" type="checkbox"/> Присутствует с использованием межсетевое экрана
<b>Как часто проходят проверки исправности устройств</b> <input type="checkbox"/> Не проходят <input checked="" type="checkbox"/> Раз в год <input type="checkbox"/> Раз в полгода <input type="checkbox"/> Раз в месяц
<b>Функционал межсетевого экрана</b> <input checked="" type="checkbox"/> Межсетевой экран с фильтрацией пакетов <input type="checkbox"/> Шлюзы свансового уровня <input type="checkbox"/> Шлюзы прикладного уровня <input type="checkbox"/> Межсетевые экраны экспертного уровня
<b>Какая антивирусная система используется</b> <input type="checkbox"/> Без сертификатов безопасности от НДВ <input checked="" type="checkbox"/> С сертификатом Безопасности от НДВ <input type="checkbox"/> С сертификатом ФСТЭК
<b>Кто имеет доступ к защищаемой системе</b> <input type="checkbox"/> Любой посетитель <input checked="" type="checkbox"/> Любой сотрудник предприятия <input type="checkbox"/> Ограниченный круг лиц

## Результаты определения уровня защищенности

Средний уровень исходной защищенности

Перейти к мерам повышения уровня защищенности

Начать заново

Вернуться в начало

Результат прохождения

анкетирования

## Меры повышения уровня защищенности

Необходимо внедрение биометрической защиты при аутентификации и идентификации

Необходимо проводить проверку неисправность устройств не реже раза в месяц

Необходима установка межсетевого экрана экспертного уровня

Необходимо использование антивирусной системы с сертификатом ФСТЭК

Допустить к защищаемой системе ограниченный круг лиц

Меры по повышению  
уровня защищенности

Угроза воздействия на программы  
с высокими привилегиями

# АПРОБАЦИЯ ИССЛЕДОВАНИЯ НА ОБЪЕКТЕ (МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ)

15

Определение степени возможного ущерба Многофункционального центра государственных и муниципальных услуг при помощи разработанного подхода.

$$\mathcal{E}_y = \mathcal{Ш}_z + \mathcal{O}_y + \mathcal{З}_в + \mathcal{З}_п, \text{ где:}$$

$\mathcal{Ш}_z = 140\,000$  рублей;

$\mathcal{O}_y = 50\,000$  рублей;

$\mathcal{З}_в = 500\,000$  рублей;

$\mathcal{З}_п = 60\,000$  рублей.

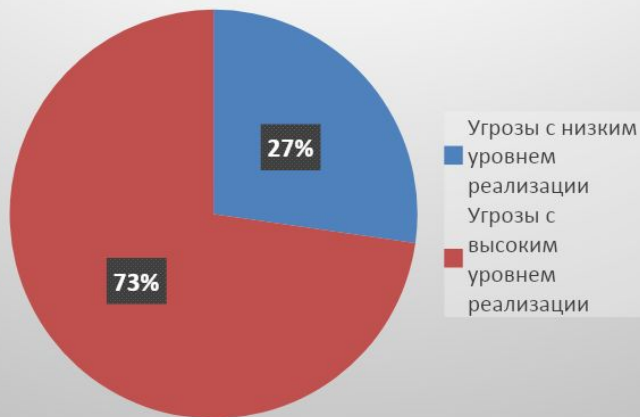
Общий ущерб:  $\mathcal{E}_y = 140\,000 + 50\,000 + 500\,000 + 60\,000 = 750\,000$  рублей.

750 000 рублей (ущерб) от 1 500 000 рублей (чистый доход) составляет 50%. Согласно ранее разработанному подходу определения степени возможного ущерба, существенные негативные последствия – ведут к выплате штрафов, компенсаций, иным затратам, составляющим от 50 до 100 % чистого дохода организации, следовательно, степень возможного ущерба **высокая**.

# АПРОБАЦИЯ ИССЛЕДОВАНИЯ НА ОБЪЕКТЕ (МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ)

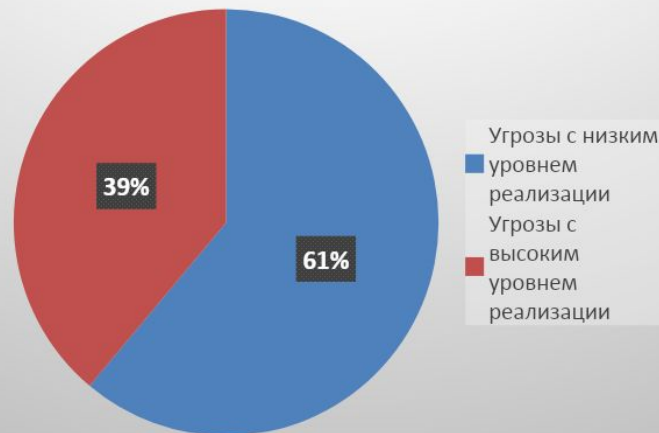
16

## Оценка защищенности



Определение уровня защищенности до применения разработанного алгоритма

## Оценка защищенности



Определение уровня защищенности после применения разработанного алгоритма

Число угроз с высоким уровнем реализации снизилось на 34%, что свидетельствует о

действенности разработанной методики.



# РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведён анализ существующей нормативно-правовой базы, методических документов и научных статей в области защиты государственных информационных систем.

2. Разработана методика определения степени возможного ущерба.

3. Разработан алгоритм определения уровня защищённости государственных информационных систем.

4. Разработан программный продукт определения степени возможного ущерба и определения уровня защищённости информационной системы.



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Брянский государственный технический университет**

**Факультет информационных технологий**

**Кафедра «Системы информационной безопасности»**

**МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ**

**по направлению подготовки 10.04.01– «Информационная безопасность»  
на тему: Разработка методики определения степени возможного ущерба  
и алгоритма определения уровня защищённости государственных  
информационных систем**

Магистрант группы: О-18-ИБ-ози-М

Клищенко Р.А.

Руководитель работы:

к.т.н., доц., Голембиовская О.М.

Брянск 2021