КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | К а л и н и н г р а д

08.06.2023

Центр защиты информации

Знакомство

Обо мне

- В 2012 году окончил Балтийский федеральный университет им. И. Канта по специальности: «Организация и технология защиты информации»
- С 2012 года работал в государственных учреждениях на различных должностях, отвечал за обеспечение информационной безопасности
- С 2013 года осуществляю преподавательскую и научную деятельность в сфере защиты информации, член государственной аттестационной комиссии.
- Руководитель и Владелец компании, занимающейся информационной безопасностью.

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как одновременно соответствовать требованиям регуляторов и обеспечивать реальную защиту информации?

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Основные нормативно-правовые акты

Конституция Российской Федирации

Федеральный закон № 149 "Об информации, информационных технологиях и о защите информации" от 27.07.2006

Федеральный закон № 152 «О персональных данных» от 27.07.2006

Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012

Постановление Правительства Российской Федерации № 687 от «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008

Постановление Правительства Российской Федерации № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 15.09.2008

Приказ ФСТЭК «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 №21

Приказ ФСБ России № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014

Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

(введена Федеральным законом от 25.07.2011 N 261-ФЗ)

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. *Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами*, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Требования к средствам защиты информации и межсетевым экранам

УЗ	СЗИ	СВТ	НДВ (актуальны угрозы 2т)	МЭ
Приказ ФСТЭК № 21 от 18.02.2013				Инф. сообщ. ФСТЭК от 28 апреля 2016 г. № 240/24/1986
4	Не ниже 6	Не ниже 6	Не ниже 4	6
3	Не ниже 6	Не ниже 5	Не ниже 4	6
2	Не ниже 5	Не ниже 5	Не ниже 4	5
1	Не ниже 4	Не ниже 5		4

Приказ ФСТЭК № 21 от 18 февраля 2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Оператор персональных данных действует по следующему алгоритму:

— определяет уровень защищенности своей ИСПДн согласно **ПП 1119**;

— выбирает все меры, которые отмечены плюсом для выбранного уровня защищенности (базовые меры);

— убирает из полученного списка меры, которые связаны с технологиями, не используемыми в ИСПДн (например, убираем меры для защиты виртуальной инфраструктуры, если средства виртуализации не используются);

— смотрит на полученный список мер и сравнивает с актуальными угрозами в модели угроз, если выбранными мерами нейтрализуются не все актуальные угрозы, добавляет в список компенсирующие меры, необходимые для нейтрализации всех оставшихся угроз;

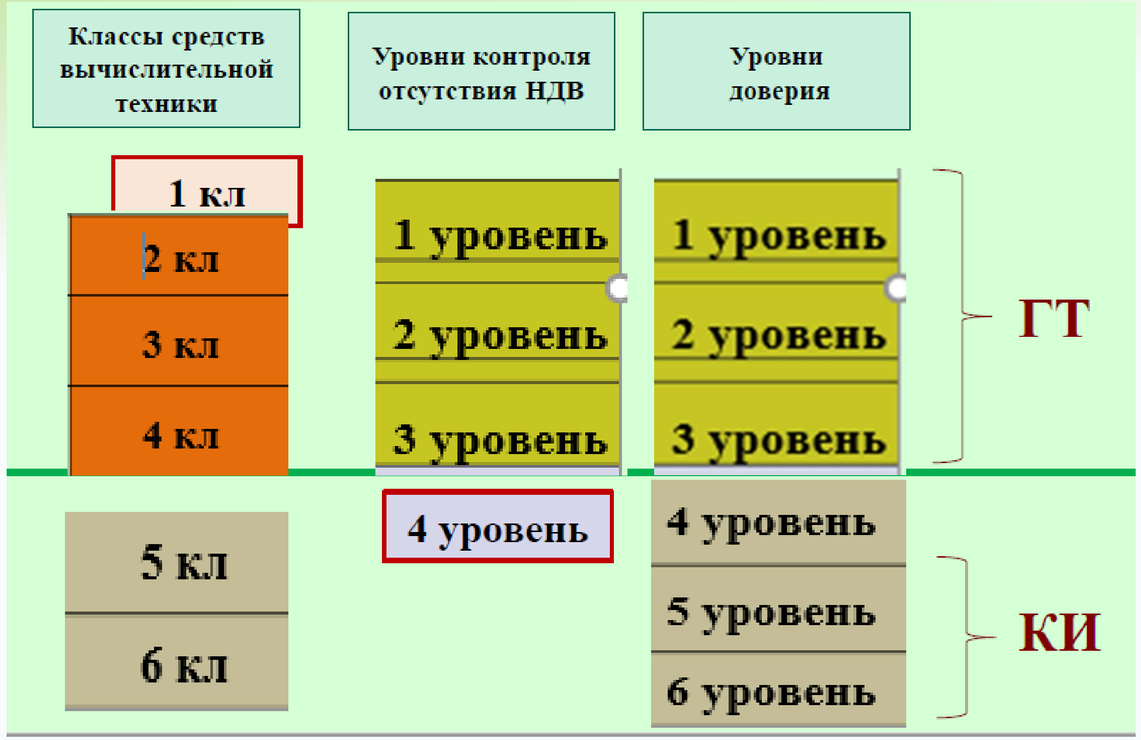
— добавляет к полученному списку меры, определенные в других нормативных актах (например в **ПП № 1119** есть небольшое количестве мер, а также есть общие требования в ФЗ-152), после чего получает итоговый список мер, которые нужно выполнить;

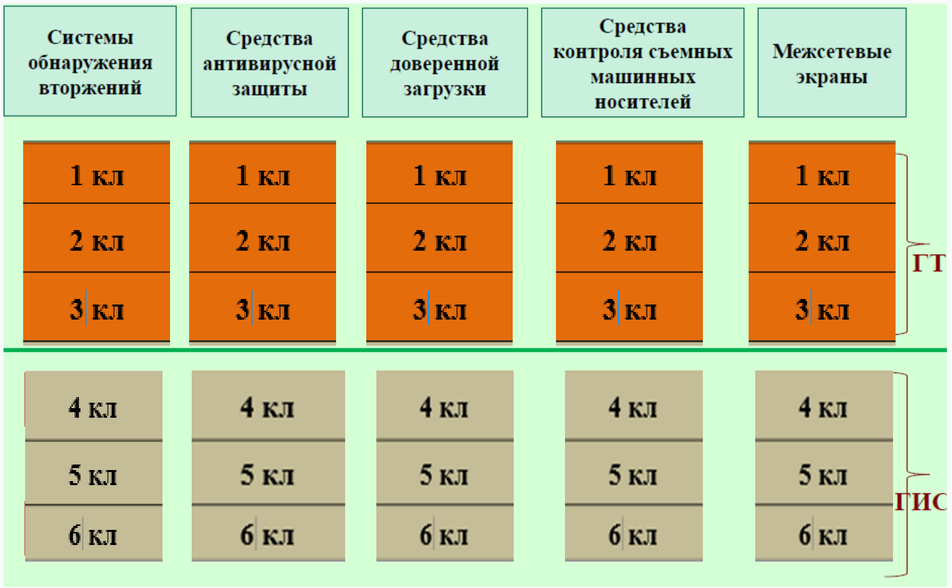
— выполняет меры из окончательного списка

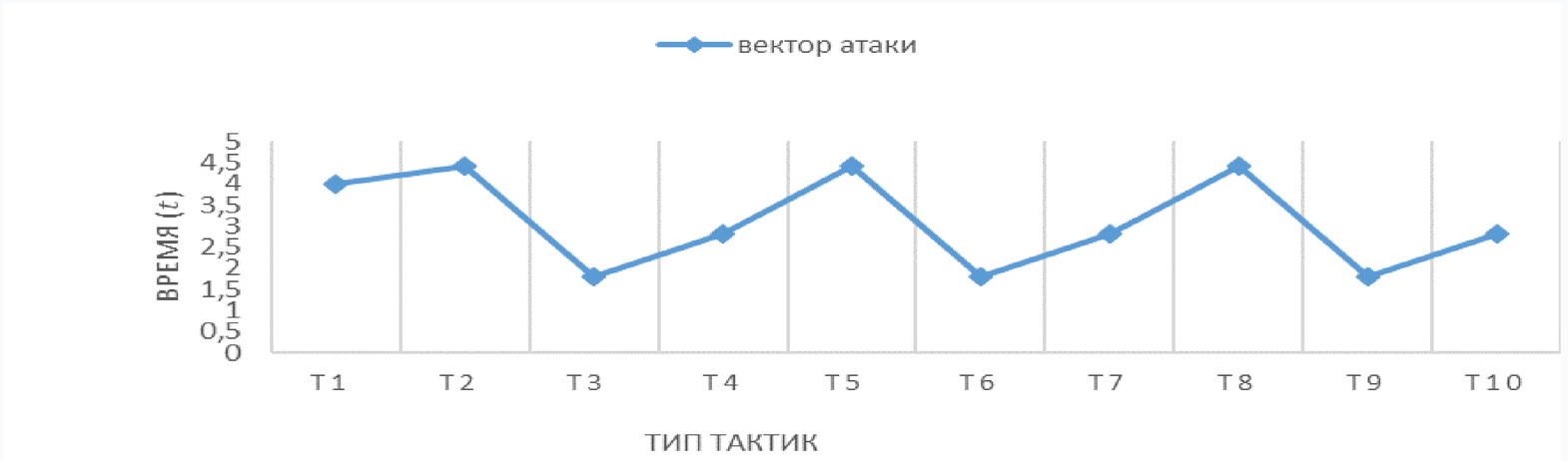
Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Атаки и классы средств защиты

Классы ГИС	Классы СЗИ
К1	4 или выше
К2	5 или выше
К3	6 или выше







КоАП РФ Статья 13.12. Нарушение правил защиты информации

6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до пятнадцати тысяч рублей.

(часть 6 введена Федеральным законом от 02.12.2013 N 341-ФЗ)

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Готов ответить на ваши вопросы

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ