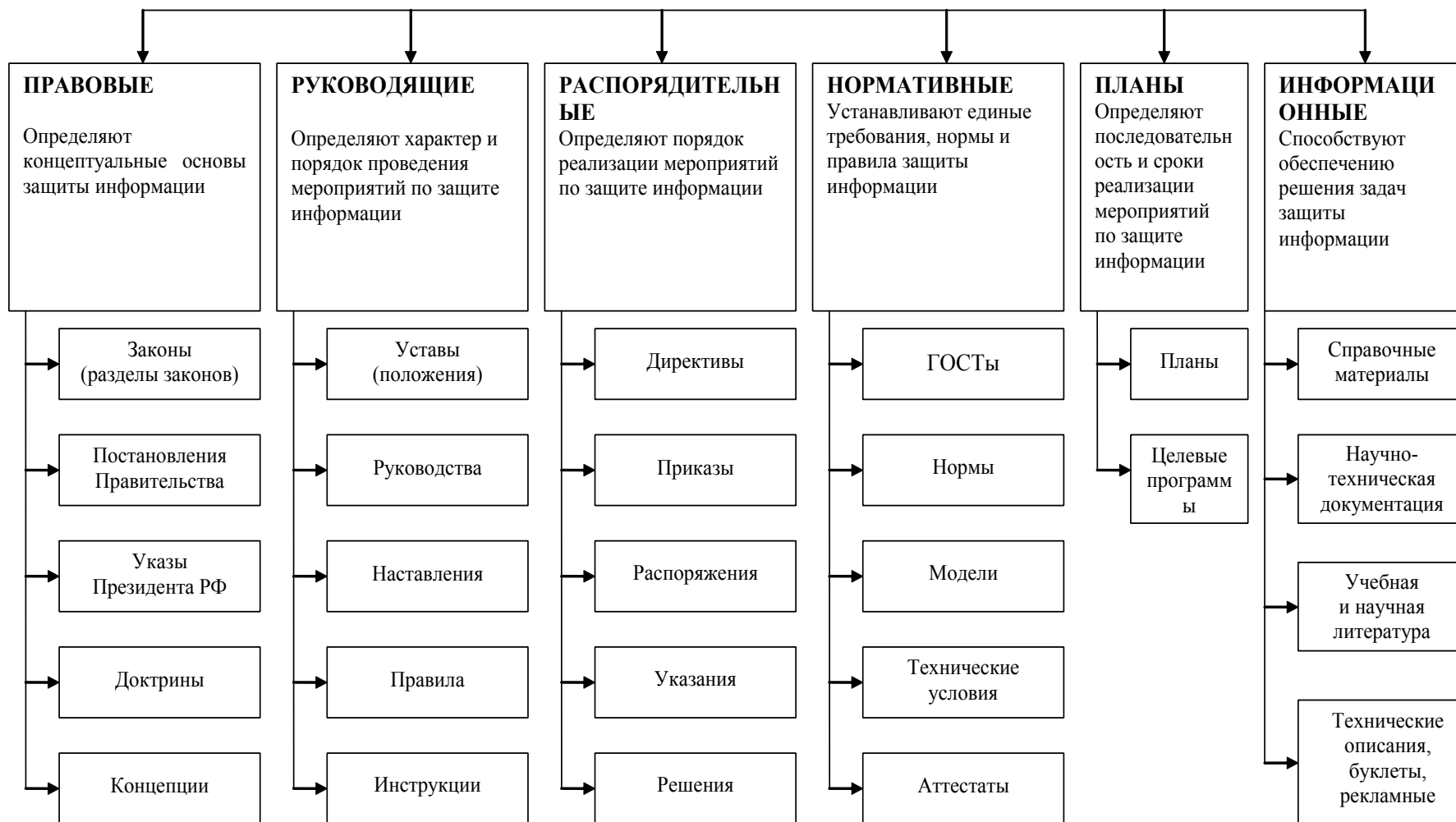


Реализация законодательства в области обеспечения безопасности КИИ: первые опыты

Атаманов Г.А.
кандидат философских наук
автор научной теории безопасности

Документы по защите информации



Общие тезисы:

- ✓В сфере ИБ/БИ/ТЗИ в РФ издано огромное количество НПА, РД и НМД, которые зачастую противоречат друг другу.
- ✓Терминология, используемая в НПА, РД и НМД в сфере ИБ/БИ/ТЗИ, сформирована с нарушениями всех известных законов логики, а парадигма, на базе которой она построена, носит ненаучный (эзотерический) характер.
- ✓Алогичность определений понятий в сфере ИБ/БИ/ТЗИ и их полисемичность не позволяют построить сколь-нибудь эффективную систему защиты информации, а об ИБ в законодательстве РФ, практически, нет речи.
- ✓Единственным критерием оценки качества СЗИ (кроме ОКИИ) является её соответствие/несоответствие требованиям НПА.
- ✓Системы защиты, построенные в соответствии с требованиями НПА, малоэффективны, громоздки и затратны, но их нужно строить, чтобы не попасть «под раздачу».
- ✓Для построения эффективных систем защиты информации целесообразно руководствоваться ISO, COBIT, NIST и «лучшими практиками».

Оценка читабельности ПП-127 о категорировании объектов КИИ:

Оценка читабельности

Очень сложно читать

Сложно

Легко

Уровень читабельности

28.1

Аудитория

Аспирантура, второе высшее образование, PhD

Индикаторы читаемости текста

Формула Flesch-Kincaid **30.76**

Индекс Колман-Лиану **24.56**

Формула Дэйла-Чейла **26.93**

Automatic Readability Index **29.66**

SMOG **28.1**

Расчётные показатели

26755 знаков

2961 пробел

22406 букв

2674 слова

91 предложение

916 слов с более чем 4-мя слогами

1758 слов до 4-х слогов включительно

29.38 слов в среднем на предложение

3.66 слова в среднем на предложение

34.26% сложных слов

Оценка читабельности текста

Текст

Веб-страница

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Принят
Государственной Думой
12 июля 2017 года

Рассчитать

Оценка читабельности

Очень сложно читать

Сложно

Легко

Уровень читабельности

32.14

Аудитория

**Аспирантура, второе высшее образование,
pHD**

Индикаторы читаемости текста

Формула Flesch-Kincaid **34.6**

Индекс Колман-Лиау **28.36**

Формула Дэйла-Чейла **30.96**

Automatic Readability Index **34.89**

SMOG **32.14**

Расчётные показатели

42002 знака

4278 пробелов

36340 букв

4018 слов

121 предложение

1594 слова с более чем 4-мя слогами

2424 слова до 4-х слогов включительно

33.21 слова в среднем на предложение

3.84 слова в среднем на предложение

39.67% сложных слов

Особенности реализации 187-ФЗ «О безопасности КИИ РФ»:

- алогичные формулировки «понятий, используемых в законе»
- запутанная и сложная технология реализации
- не назначен орган госвласти, ответственный за трактовку положений
- алогичные требования к СЗ объектов КИИ
- трудности в подключении к ГосСОПКА
- подследственность ФСБ
- необходимость «самозаклада» в случае инцидента
- серьёзные штрафы за нарушение требований НПА
- уголовная ответственность не только для злоумышленника, но и для субъекта КИИ
- избирательная правоприменительная практика

Если вы думаете, что ваше предприятие не субъект КИИ, то не факт, что вы правы.

Если вы провели категорирование объектов КИИ, то вы однозначно сделали это неправильно.

Если вы разработали Модель угроз безопасности информации в КИИ, то:

- а) с точки зрения обеспечения безопасности объекта КИИ это абсолютно бесполезный документ;
- б) с точки зрения логики этот документ всегда неправильный.

Если у вас до настоящего времени не было серьёзных инцидентов с ИТКС и ИР, то не факт, что их не будет и завтра.

В РФ нет прецедентного права, поэтому если вашего знакомого оштрафовали за непринятие мер по защите ИС/ИТКС/АСУ или несвоевременный доклад об инциденте, то не факт, что и вас тоже только оштрафуют.

Ответственность для тех кто «взламывает»

Деяние	Наказание
Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ...	До 5 лет л/с штраф до 1 млн. руб.
Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ...	До 6 лет л/с штраф до 1 млн. руб.
Совершено группой лиц	До 8 лет л/с



Ответственность для тех кто обслуживает и защищает

Деяние	Наказание
Нарушение правил эксплуатации [ИТ] КИИ..., если оно повлекло причинение вреда КИИ	До 6 лет л/с
С тяжкими последствиями	До 10 лет л/с



УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Уголовный кодекс Российской Федерации
№ 63-ФЗ от 13.06.1996 (ред. от 27.10.2020)

- Статья 272. Неправомерный доступ к компьютерной информации
- Статья 273. Создание, использование и распространение вредоносных компьютерных программ
- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
- **Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации**

В конце 2019 года к проверке выполнения 187-ФЗ подключилась прокуратура. По стране прошёл массовый запрос сведений от организаций:



ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА

ТРЕБОВАНИЕ

в порядке ст.ст. 6, 22 Федерального закона от 17.01.1992 № 2202-1 «О прокуратуре Российской Федерации»

Прокуратурой города [REDACTED] проводится проверка в сфере безопасности использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации.

На основании вышеизложенного и в соответствии со ст.ст. 6, 22 Федерального закона от 17.01.1992 № 2202-1 «О прокуратуре Российской Федерации» прошу Вас не позднее 18-00 часов 22.01.2020 представить в прокуратуру города следующие сведения за период с 2018 по 2019 годы (с приложением подтверждающих документов):

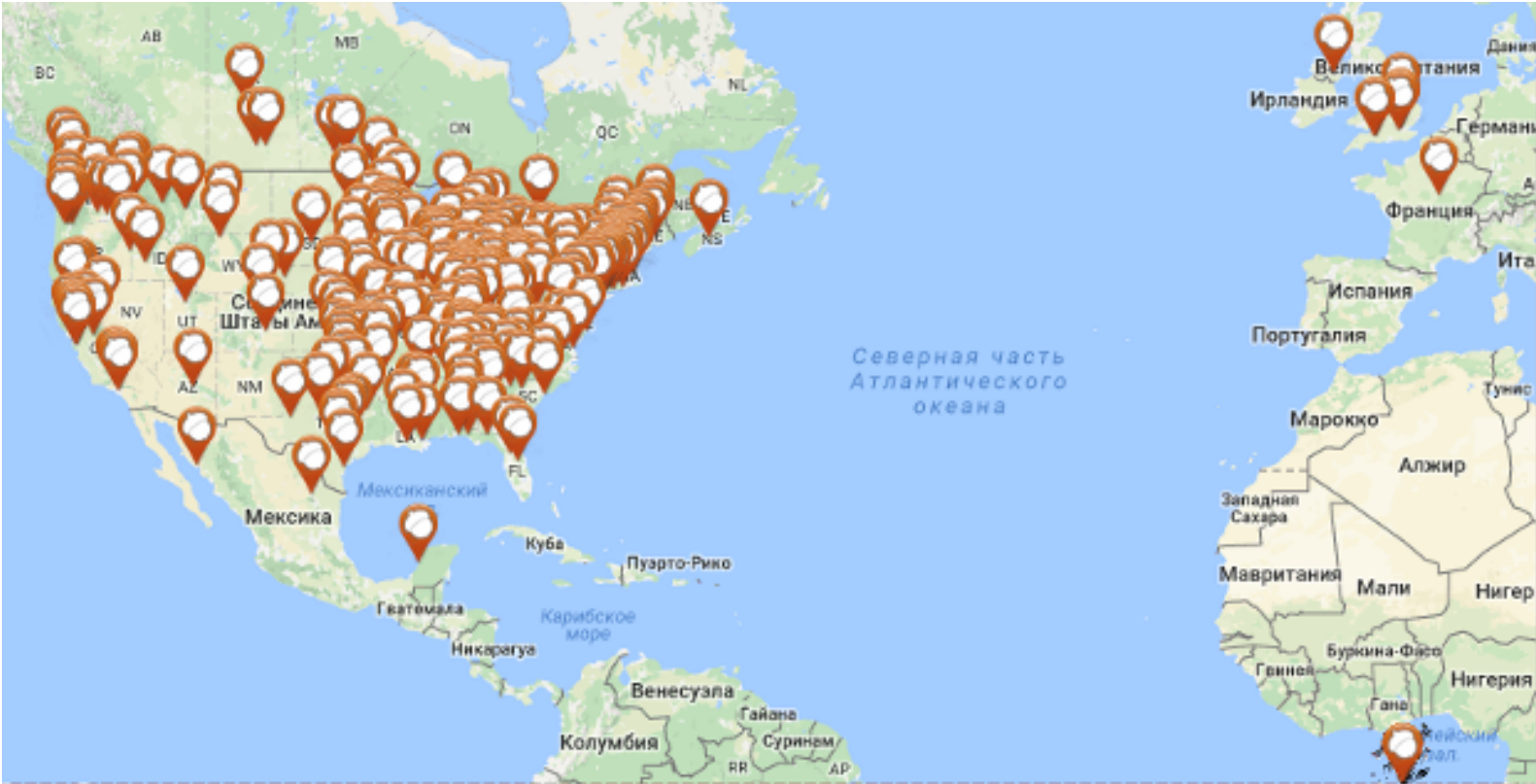
- сведения о местах размещения сооружений, средств и сетей связи, обеспечения их защиты; сведения о государственной регистрации права собственности и других вещных прав на объекты связи; сведения об установлении тарифов на услуги связи; сведения о наличии лицензии на осуществление деятельности; сведения о сертификации средств и услуг связи; сведения о хранении баз данных об абонентах;
- сведения о наличии ограничений доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в России запрещено;
- сведения о наличии статуса субъекта критической информационной инфраструктуры;
- сведения о присвоении категории значимости объекту критической информационной инфраструктуры;
- сведения о создании системы безопасности значимых объектов критической информационной инфраструктуры;
- сведения о соблюдении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Разъясняю, что за невыполнение требований прокурора, вытекающих из его полномочий, в том числе за нарушение срока предоставления ответа или неполноты ответа Вы можете быть привлечены к административной ответственности в соответствии со ст.17.7 КоАП РФ.

Судебные дела по 187-ФЗ КИИ

№	Часть	Судебное дело	Приговор	Примечание
1	ч.1.	1-345/2019 от 31.05.2019 г. Петропавловск-Камчатский	от уголовной ответственности освободить	В связи с деятельным раскаянием.
2	ч.1	1-337/2019 от 16.08.2019 г. Волгоград	судебный штраф	Добровольное возмещение ущерба
3	ч.4	1-368/2019 от 25.09.2019 г. Владивосток	3 года условно	Работник субъекта КИИ
4	ч.4	1-376/2019 от 25.09.2019 г. Владивосток	2 года условно	Явка с повинной, добровольное возмещение ущерба (3 человека)
5	ч.1	1-170/2020 от 24.04.2020 г. Волгоград	-	Возвращено прокурору
6	ч.4	1-536/2020 от 26.06.2020 г. Благовещенск	3 года условно	Работник субъекта КИИ
7	ч.1	1-251/2020 от 17.07.2020 г. Волгоград	судебный штраф	
8	ч.2	1-805/2020 от 14.07.2020 г. Абакан	2 года условно	Работник субъекта КИИ
9	ч.1	1-268/2020 от 05.10.2020 г. Кемерово	3 года условно	Подбор паролей к сети предприятия ОПК, вреда нет
10	ч.1	1-353/2020 от 06.10.2020 г. Волгоград	2 года условно	Работник субъекта КИИ
11	ч.1	1-315/2020 от 16.10.2020 г. Волгоград	2 года условно	Работник субъекта КИИ
12	ч.1	1-110/2020 от 24.11.2020 г. Волгоград	Судебный штраф – 15 000 руб.	Работник субъекта КИИ
13	ч.2	1-339/2020 от 07.12.2020 г. Волгоград	2 года условно	Работник субъекта КИИ
14	ч.3	№ 1-1317/2020 от 07.12.2020 г. Благовещенск	приговор	Возможно 3 года условно, см.№6
15	ч.1	1-343/2020 от 10.12.2020 г. Волгоград	приговор	
16	ч.2	1-395/2020 от 20.01.2021 г. Волгоград	приговор	
17	ч.4	1-458/2020 г. Владикавказ	?	ждем
18	Ч.4	1-88/2021 от 19.02.2021 г. Иваново	3 года условно	Работник субъекта КИИ

что белки представляют более серьёзную опасность для инфраструктуры, чем «кибератаки» хакеров.



Районы, где белки нанесли ущерб линиям электропередач

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях её устойчивого функционирования при проведении в отношении её компьютерных атак.

Ст. 1. 187-ФЗ



В. Винокур: «Здесь играем, здесь играем, здесь я рыбу заворачивал...»



Если названия вещей не точны, их словесное выражение не отражает сути. Если слова не отражают сути, дела не могут быть завершены. Незавершение дел выхолащивает ритуал и музыку. Умаление значения музыки и обычаев приводит к тому, что наказание не достигает цели. Если наказание не действенно, общество ожидает хаос. Поэтому, если благородный человек о чем-то говорит, его слова должны нести чёткую смысловую нагрузку, ибо слова не должны расходиться с делом.

В своих высказываниях благородный человек должен проявлять определённую, но не небрежность.

Конфуций
6 век до н.э.

**«Теория без практики
мертва и бесплодна,
практика без теории
бесполезна и пагубна»**

**Великий математик,
Пифагорий Чебышев**



БЕРЕГИТЕ:

- СЕБЯ (здоровье, свободу, сознание);**
- СВОИХ РОДНЫХ И БЛИЗКИХ;**
- СВОЁ ИМУЩЕСТВО И СВОЙ БИЗНЕС;**
- СВОИ ИНФОРМАЦИОННЫЕ РЕСУРСЫ!**

Атаманов Г.А.

g.a.atamanov@yandex.ru

<http://gatamanov.blogspot.ru>