Федеральное государственное бюджетное образовательное учреждение высшего образования

«Новосибирский государственный технический университет»

Кафедра защиты информации

УТВЕРЖДАЮ
Заведующий ОПКВК
_____ В. П. Драгунов
«21» марта 2022 г.

ПРОГРАММА

вступительного экзамена в аспирантуру по специальности

2.3.6 Методы и системы защиты информации, информационная безопасность

Новосибирск – 2022

Программа обсуждена на заседании кафедры защиты информации, протокол заседания кафедры № 2 от 14.02. 2022 г.

Утверждена на заседании ученого совета факультета автоматики и вычислительной техники № 3 от 16.03. 2022 г.

Ответственный за образовательную программу:

к.т.н., доцент А. В. Иванов

Заведующий кафедрой:

к.т.н., доцент А. В. Иванов

Декан АВТФ:

к.т.н., доцент И.Л. Рева

Программа вступительных испытаний по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» содержит перечень экзаменационных вопросов и список рекомендуемой литературы. В основу программы вступительных испытаний положены следующие дисциплины: Безопасность операционных систем, Программно-аппаратные средства обеспечения информационной безопасности, Безопасность сетей электронных вычислительных машин, Организационное и правовое обеспечение информационной безопасности, Защита информации от утечки по техническим каналам, Технические средства охраны объектов, Комплексная защита объектов информатизации, Безопасность систем баз данных.

Вопросы к вступительному экзамену

1. Информация, сообщение, информационные системы и процессы как объекты информационной безопасности. Основные свойства информации. Мера количества информации. Энтропия. Модели стоимости информации.
2. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события. Условная вероятность. Формула полной вероятности. Теорема Байеса.
3. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
4. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
5. Математические модели: виды, возможности, ограничения, области применения. Современные инструментальные средства математического моделирования.
6. Виды угроз безопасности информации.
7. Источники угроз безопасности информации.
8. Лицензирование в области защиты информации.
9. Сертификация в области защиты информации.
10. Основные понятия Закона РФ "О государственной тайне". Перечень сведений, составляющих государственную тайну.
11. Организация доступа к государственной тайне.
12. Конфиденциальная информация. Основные понятия.
13. Организация доступа к конфиденциальной информации.
14. Аттестация объектов информатизации по требованиям безопасности информации. Общие положения.

15. Организация защиты конфиденциальной информации на объектах информатизации. Общие положения.
16. Безопасность ИСПДн.
17. Безопасность ГИС, МИС.
18. Безопасность КИИ.
19. Безопасность АСУ ТП.
20. Модели безопасности БД.
21. Управление доступом к БД.
22. Уровни разграничения доступа к БД.
23. SQL-инъекции. Способы реализации и защиты.
24. XSS-уязвимости. Способы обнаружения и борьбы с ними.
25. Модель OSI, стек TCP/IP, уровни, примеры протоколов и их назначение.
26. Протоколы маршрутизации.
27. Технологии VLAN, DNS, DHCP.
28. Технологии NAT, PAT.
29. Технология VPN, определение, классификация, примеры протоколов.
30. Основная методология безопасности в области веб-технологий.
31. Различие хеширования и шифрования.
32. SSL и HTTPS. Различие принципы реализации и оценки безопасности.
33. Виды резервного копирования информации и их описание
34. Виды вредоносного программного обеспечения
35. Способы распространения вредоносного программного обеспечения
36. Ответственность за правонарушения в области информационной безопасности.
37. Контролирующие органы государственной власти в области информационной безопасности и их полномочия.
38. Международное законодательство в области обеспечения информационной безопасности.
39. Классификация технических каналов утечки информации.
40. ТКУИ в защищаемом помещении.
41. ТКУИ в автоматизированных системах.
42. Виды и методы защиты информации от утечки по техническим каналам.
43. Системы контроля и управления доступом.
44. Системы видеонаблюдения.
45. Системы охранно-пожарной сигнализации.
46. Программно-аппаратные средства защиты информации. Классификация.
47. Межсетевые экраны.

48. Средства защиты информации от несанкционированного доступа.
49. Средства доверенной загрузки.
50. Криптошлюзы.
51. Системы обнаружения и предотвращения вторжений (IDS/IPS).
52. Различия IDS и IPS в контексте кибербезопасности
53. Антивирусные средства защиты.
54. Средства мониторинга событий информационной безопасности.
55. Виды мониторинга трафика.
56. Виды фильтрации трафика.
57. Основные типы кибератак.
58. Тестирование на проникновение, назначение, виды, результаты.
59. Процедура проведения аудита ИС.
60. Расследование и реагирование на инциденты ИБ.
61. ГосСОПКА. НКЦКИ.
62. Безопасность операционных систем. Защищенные ОС.
63. Средства аутентификации и разграничения доступа.
64. Системы предотвращения утечки информации (DLP).
65. Криптографические методы защиты информации. Основные понятия
66. Классификация алгоритмов шифрования. Примеры простейших шифров.
67. Синхронное и асинхронное шифрование
68. Средства криптографической защиты информации. Порядок обращения с СКЗИ.
69. Аппаратные токены ЭЦП. Основные механизмы. Удостоверяющие центры. Инструменты.
70. Международное законодательство в области информационной безопасности.

Правила аттестации

Оценка знаний поступающего в аспирантуру осуществляется в ходе экзамена, проводимого в письменной форме по билетам, составляемым по вопросам, соответствующим разделам представленной выше программы. В каждом билете содержатся три вопроса.

По результатам ответов на вопросы билета, поступающий в аспирантуру может получить следующие оценки:

- «отлично», если на все три вопроса билета даны исчерпывающие и правильные ответы, либо ответ на один вопрос правильный, но недостаточно полный;

- «хорошо», если ответы на вопросы правильные, но недостаточно полные (например, раскрыта суть рассматриваемой проблемы, но не приведены примеры), или на два вопроса билета дан исчерпывающий и правильный ответ, а на один из вопросов билета дан не вполне правильный ответ.

- «удовлетворительно», если лишь на один из вопросов билета дан достаточно полный и правильный ответ, в то время как на другие вопросы экзаменуемый дал не вполне правильные ответы (содержащие фрагментарные знания);

- «неудовлетворительно», если на все три вопроса билета поступающий в аспирантуру представил неправильные ответы (либо ответы, содержащие лишь фрагментарные знания).

Основная литература

1. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=315649 - Загл. с экрана.
2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. - 140 с. - ISBN 978-5-9275-3546-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1308349 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=374990 - Загл. с экрана.
3. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин. - Москва : РИОР : ИНФРА-М, 2020. - 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1118462 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/product/1118462 - Загл. с экрана.
4. Гвоздева, В. А. Основы построения автоматизированных информационных систем : учебник / В. А. Гвоздева, И. Ю. Лаврентьева. — Москва : ФОРУМ : ИНФРА-М, 2020. — 318 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0705-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1066509 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=350418 - Загл. с экрана.
5. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. -

(Высшее образование: Специалитет). - Текст : электронный. - URL: https://znanium.com/catalog/product/1178150 (дата обращения: 23.08.2021). – Режим доступа: по подписке.

6. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 23.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/product/1210523 - Загл. с экрана.

7. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 23.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/product/463037 - Загл. с экрана.

8. Иванов А. В. Оценка защищенности информации от утечки по виброакустическим каналам : [учебное пособие] / А. В. Иванов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2018. - 74, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000239301

9. Иванов А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : [учебное пособие] / А. В. Иванов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2018. - 63, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000239355

10. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 23.08.2021). – Режим доступа: по подписке.

11. Костин, В. Н. Методы и средства защиты компьютерной информации : криптографические методы для защиты информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 40 с. - ISBN 978-5-90695-334-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232230 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=371043 - Загл. с экрана.

12. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021744 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=339855 - Загл. с экрана.

13. Основы технологий баз данных: учебное пособие / Б. А. Новиков,Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. — 2-е изд. — М.:ДМК Пресс, 2020. — 582 с.

14. Weikum G., Vossen G. Transactional Information Systems: Theory, Algorithms, and the Practice of Concurrency Control and Recovery. — Morgan Kaufmann, 2002. — ISBN 1-55860-508-8.

15. Калашников А.О., Ермилов Е.В., Чопоров О.Н., Разинкин К.А. Баранников Н.И. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков. Под ред. чл.-корр. РАН Д.А Новикова. – Воронеж: Издательство «Научная книга», 2013. – 160 с.

16. Эндрю Хоффман. Безопасность веб-приложений. – Издательский дом «Питер», 2021. – 336с.

17. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с

18. Зегжда Д. П., Александрова Е. Б., Калинин М. О., Марков А. С., Жуков И. Ю , Иванов Д. В., Коноплев А. С., Лаврова Д.С., Москвин Д. А., Павленко Е. Ю., Полтавцева М. А., Шенец Н. Н., Дахнович А. Д., Крундышев В. М. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. - Горячая Линия - Телеком, 2020. – 560 с

19. Брюс Шнайдер. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – Далекива, 2017. – 1040 с.

20. Иван Ристич. Пуленепробиваемые SSL и TLS. Издательство: Feisty Duck, 2014. – 568 с.

21. Сухомлин В.А., Белякова О.С., Климина А.С.,Полянская М.С., Русанов А.А. Модель цифровых навыков кибербезопасности / Фонд Лига интернет-медиа, 2021 - 294 стр.

22. А.С. Мухаммад. Сканер уязвимостей SQL. – Издательство: Sciencia scripts, 2021. – 144 с.

Дополнительная литература

1. Введение в информационную безопасность и защиту информации : [учебное пособие / В. А. Трушин и др.] ; Новосиб. гос. техн. ун-т. - Новосибирск, 2017. - 130, [2] с. : ил.. табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235435

2. Жуков, В. Г. Беспроводные локальные сети стандартов IEEE 802.11 a/b/g [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 128 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463047 (дата обращения: 23.08.2021). – Режим доступа: по подписке.

3. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 23.08.2021). – Режим доступа: по подписке.

4. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244 (дата обращения: 23.08.2021). – Режим доступа: по подписке.

5. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178151 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/product/1178151 - Загл. с экрана.

6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/product/1137902 - Загл. с экрана.

7. Котов Ю. А. Приложения шифров. Криптоанализ : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2019. - 74, [2] с. : схемы, табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000241161

8. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1036519 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=343296 - Загл. с экрана.

9. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=368272 - Загл. с экрана.

10. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 24.08.2021). – Режим доступа: по подписке. - Режим доступа: https://znanium.com/catalog/document?id=371348 - Загл. с экрана.

11. Басыня Е. А. Операционные системы : учебно-методическое пособие / Е. А. Басыня, А. В. Сафронов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 82, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000233803

12. Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012

13. Зырянов С. А. Информационная безопасность в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2018]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000237649. - Загл. с экрана.

14. Зырянов С. А. Основы информационной безопасности в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2021]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000243905. - Загл. с экрана.

15. Иванов А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : [учебное пособие] / А. В. Иванов, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2012. - 40, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000167975

16. Муртазина М. Ш. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / М. Ш. Муртазина ; Новосиб. гос. техн. ун-т. - Новосибирск, [2020]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000243237. - Загл. с экрана.

17. Туманов С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 54, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000227592

18. Туманов С. А. Система защиты информации от несанкционированного доступа на основе "SecretNet 7" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 89, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000226348

Интернет-источники

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/

2. Федеральной службой безопасности Российской Федерации (ФСБ РФ) http://www.fsb.ru/

3. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций https://rkn.gov.ru/

4. Росстандарт https://www.rst.gov.ru/portal/gost

5. The National Institute of Standards and Technology, NIST https://www.nist.gov
6. Open Web Application Security Project https://owasp.org/
7. Barkeley Information Security Office https://security.berkeley.edu/

Перечень основных нормативно-методических документов

1. Приказ ФАПСИ от 13.06.2001 № 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»
2. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
3. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных».
4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».
6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Приказ ФСБ России от 10.07.2014 № 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»
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
10. Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».
11. Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»
12. Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

13. Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

14. Указ Президента РФ №569 от 25.11.2017 «О внесении изменений в Положение о ФСТЭК»

15. Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»

16. Приказ ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

17. Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

18. Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

19. Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

20. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

21. Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

22. Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»

23. Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

24. Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

25. Приказ ФСБ России №196 от 06.05.2019 «Об утверждении требований к средствам ГосСОПКА»

26. Приказ ФСБ России №281 от 19.06.2019 «Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА»

27. Приказ ФСБ России №282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗО КИИ РФ»

28. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1

29. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ

30. Приказ Федеральной службы безопасности Российской Федерации от 27.12.2011 № 796 г. Москва «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».