**Safe Digit**

**Оглавление**

[**Персонал SOC** 3](#_Toc56311309)

[**Оценки эффективности будущего SOC** 4](#_Toc56311310)

[**Этапы создания SOC и выбор технологий** 5](#_Toc56311311)

[**Подготовительный этап** 5](#_Toc56311312)

[**Этап 1** 5](#_Toc56311313)

[**Этап 2** 5](#_Toc56311314)

[**Этап 3** 6](#_Toc56311315)

[**Этап 4** 6](#_Toc56311316)

[**Этап 5** 7](#_Toc56311317)

[**Перспективы** 8](#_Toc56311318)

[**Социальный эффект** 9](#_Toc56311319)

[**Социальное воздействие / социальный эффект (Impact)** 9](#_Toc56311320)

[**Непосредственные результаты** 9](#_Toc56311321)

[**Социальные результаты** 9](#_Toc56311322)

[**Социальное воздействие** 9](#_Toc56311323)

[**Мы можем обеспечить:** 9](#_Toc56311324)

[**Временные показатели** 10](#_Toc56311325)

[**Сроки, определённые кейсодержателем:** 10](#_Toc56311326)

[**В целях первичного развёртывания системы необходимо (до середины 2-го квартала 2021):** 10](#_Toc56311327)

[**В целях сокращения времени первичного развёртывания необходимо:** 10](#_Toc56311328)

[**В целях финального развертывания всех ветвей системы и выхода на расчётную эффективность работы (до конца 4-го квартала 2021 года) необходимо:** 11](#_Toc56311329)

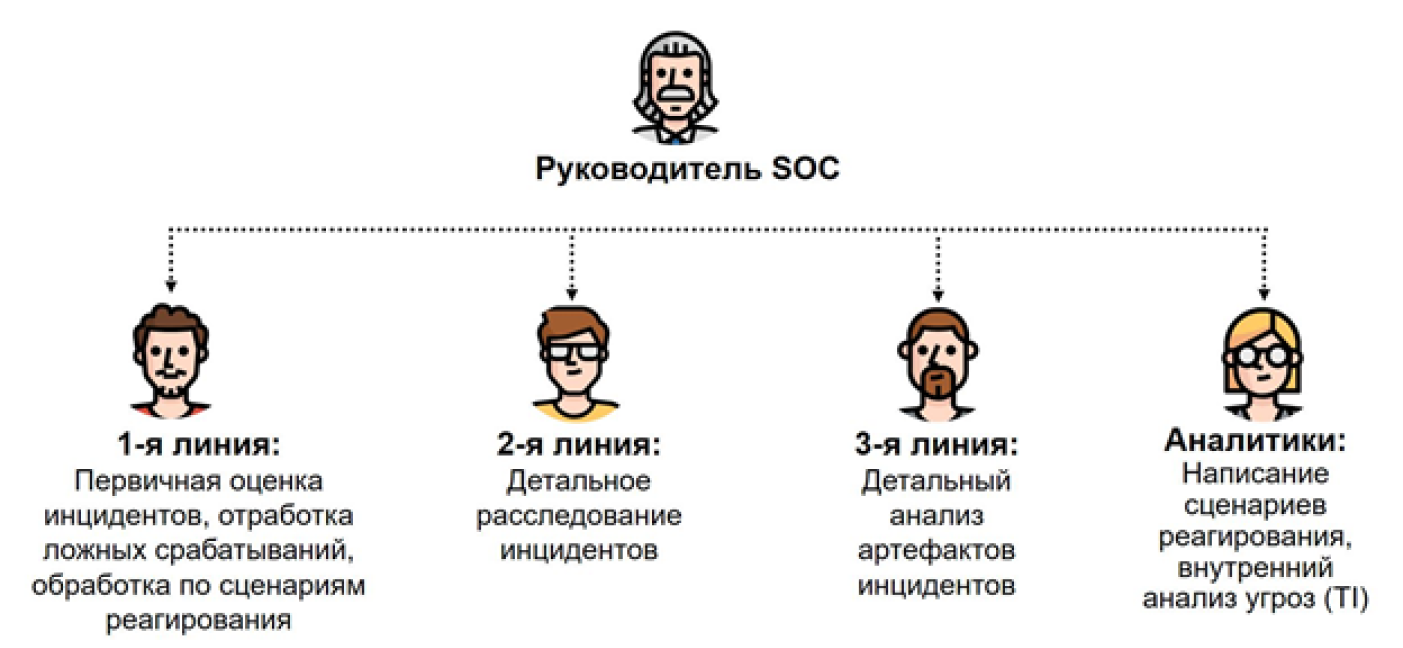
[**В целях сокращения времени на финальном этапе необходимо:** 11](#_Toc56311330)

[**Таким образом, расчетное время для начала функционирования системы – лето 2021, итоговая готовность – конец 2021** 11](#_Toc56311331)

[**База НПА** 14](#_Toc56311332)

**Услуги**

# **Персонал SOC**

Руководитель SOC. Главное ответственное лицо за работу центра. Управляет реестром инцидентов и отчетов по ним. Контролирует написание регламентов и инструкций в рамках процесса. Распределяет нагрузку на специалистов и контролирует выполнение SLA при его наличии.   
Первая линия. Сотрудники, непосредственно занимающиеся мониторингом, обработкой ложных срабатываний, первичным анализом в рамках типовых сценариев реагирования (playbook). Такие сценарии помогают специалистам SOC быстро принимать решения по типовым ситуациям. Сотрудники первой линии эскалируют инцидент на вторую линии при необходимости.   
Вторая линия. Сотрудники принимают оповещения об инцидентах от первой линии и занимаеюся детальным расследованием инцидентов.   
Третья линия. Сотрудики занимаются глубоким анализом инцидентов, разбором деталей и артефактов. Могут использовать сложную аналитику, включая reverse engineering приложений.   
Аналитики. Занимаются корректировкой действующий правил корреляции, написанием и актуализацией сценариев реагирования.   
Рекомендательная система: Сотрудники занимаются разработкой и обучением нейронной сети для автоматической выдачи   


Рекомендательная система:

Разработка и обучение  
нейронной сети для   
выдачи указаний  
(инструкций)

# **Оценки эффективности будущего SOC**

Для оценки эффективности работы SOC могут применяться различные метрики, например:   
время обнаружения инцидента;   
количество инцидентов в работе у конкретного специалиста;   
время закрытия (локализации) инцидента;   
отношение закрытых открытых инцидентов.   
Но прежде всего это время реакции (SLA) и оценка с финансовой точки зрения – какой ущерб мог быть нанесен организации, если бы SOC вовремя не выявил атаку и не блокировал ее.   
Для оценки эффективности созданного Security Operation Center также необходимо проводить тренировки, в рамках которых можно использовать внешнее и внутреннее тестирование на проникновение, то есть этичный хакинг c практической реализацией атак. В рамках тестирования на проникновение можно оценить работу SOC, понять реально ли были закрыты те векторы атак, которые реализуют риски для организации. После чего устранить недостатки и усовершенствовать стратегию развития системы информационной безопасности.   
Результатом такой тренировки является оценка состояния защищенности информационных систем как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты.   
Регулярная оценка эффективности SOC позволяет достичь максимальных ключевых показателей устойчивости бизнеса и обеспечить бесперебойное функционирование критичных информационных систем организации.

# **Этапы создания SOC и выбор технологий**

## **Подготовительный этап**

Задачами на данном этапе являются:   
инвентаризация внешних компонентов информационных систем;   
анализ типовых уязвимостей внешних компонентов информационных систем.   
В результате данного этапа SOC узнает о «белых пятнах» на периметре, а также о том, как выглядит ИТ-инфраструктура снаружи для внешнего нарушителя.   
Для реализации этапа в основном применяются средства анализа защищенности (сканеры безопасности и средства инвентаризации с возможностью автоматического сравнительного анализа данных в разные периоды времени).

## **Этап 1**

После инвентаризации и выявления слепых зон на периметре предлагается реализовать меры по усилению защиты периметра, а именно:   
выявление атак на периметре;   
выявление вредоносного ПО на периметре;   
обнаружение атак на публичные сервисы.   
Результатом этапа является защита периметра от наиболее актуальных векторов атак внешнего нарушителя — от веб-атак, атак на электронную почту и атак через пользовательский трафик.   
Для реализации этапа применяются средства анализа сетевого трафика, средства защиты веб-приложений, а также средства выявление вредоносного ПО для анализа файлов, поступающих из внешних источников (почтовый и сетевой трафик).

## **Этап 2**

После инвентаризации и усиления защиты периметра выполняют следующие задачи:   
инвентаризация и выявление уязвимостей внутренних информационных систем;   
выявление вредоносного ПО внутри инфраструктуры;   
выявление следов компрометации во внутренней инфраструктуре;   
анализ событий безопасности и выявление инцидентов.   
Результатом реализации этапа является:   
создание и автоматическое обновление полной картины ИТ-инфраструктуры и бизнес-активов организации;   
автоматический анализ событий и выявление инцидентов в ИТ-инфраструктуре.   
Для автоматизации указанных задач используются:

* Средства анализа сетевого трафика.
* Средства анализа защищенности.
* Средства выявления вредоносного ПО.

Средства сбора событий безопасности и выявления инцидентов класса SIEM. Данное средство помогает решить следующие задачи:   
проследить за событиями со всех возможных источников событий за счет нормализации;   
сопоставить события безопасности в определенную последовательность (корреляция);   
сохранить события безопасности для расследований и ретроспективного анализа.   
Средства поведенческого анализа пользователей (User and Entity Behavior Analytics) для анализа отклонений от среднестатистических данных полученных за долгое время.   
Чтобы детектировать события на конечных узлах пользователей и серверах в ИТ инфраструктуре может быть использовано средство класса EDR (Endpoint Detection and Response), которое может детальнее анализировать происходящее на уровне операционной системы. EDR может выступать источником событий для SIEM системы.   
Все указанные средства выступают в качестве источников данных для SIEM. Таким образом работа группы реагирования организуется в режиме единого окна.

## **Этап 3**

Следующим этапом решаются задачи:   
формализация процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на контролируемые информационные ресурсы;   
проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;   
проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;   
организация процессов реагирования, ликвидации последствий и устранения причин компьютерных инцидентов;   
взаимодействие с вышестоящим регулятором или отраслевым CERT (Computer Emergency Response Team) при необходимости обмена информацией об атаках (с возможностью обратиться за помощью).   
Результатом реализации этапа является организация взаимодействия с регуляторами и/или CERT-ами, в том числе для выполнения требований действующего законодательства.   
Для автоматизации указанных задач используются решения класса IRP (Incident Response Platform) или более продвинутое решение класса SOAR (Security Orchestration, Automation and Response), а также средства взаимодействия с CERT-ами и государственными регуляторами (порталы, средства взаимодействия по API и др.).

## **Этап 4**

В рамках данного этапа решаются следующие задачи:.

1. анализ исходного кода (при условии наличия критичных веб-приложений, как внутренних, так и внешних) для построения цикла безопасной разработки;
2. ретроспективный анализ сетевого трафика, событий, и передаваемых по сети файлов;
3. динамический анализ файлов в инфраструктуре и на периметре на наличие ВПО;
4. оценка соответствия требованиям корпоративных, отраслевых или международных стандартов;
5. расследование инцидентов;
6. создание процесса Threat hunting.

Результаты реализации Этапа 4:   
снижены риски взлома веб-приложений и инфраструктуры в целом;   
выстроен процессный подход к расследованию и выявлению атак;   
инфраструктура соответствует внешним и внутренним стандартам ИБ.   
Для реализации этапа, помимо средств, применяемых на предыдущих стадиях, используются:

* Средства поведенческого анализа файлов («Песочницы»).
* Средства оценки соответствия.
* Средства учета и обработки угроз (Threat Intelligence).
* Средства анализа сетевого трафика в ретроспективных режимах.
* Средства анализа исходного кода.
* Средства обработки Больших данных (big data), включая машинное обучение.

**Этап 5**

Следующий этап предусматривает обучение специалистов SOC с низкой квалификацией (при расширении штата часто на первую линию набирают специалистов, которые только закончили институт) по следующим направлениям:

* обучение реагированию на инциденты;
* обучение расследованию инцидентов.

Кроме того, на данном этапе должны проводится совместные киберучения между специалистами для повышения эффективности реагирования и выработки совместных сценариев для оперативной обработки. Процесс совершенствования навыков позволит при возникновении критических ситуаций в реальной обстановке оперативно реагировать на инциденты и атаки, блокировать распространение угроз и ликвидировать последствия.   
Результатом Этапа 5 являются:

* повышение уровня экспертизы сотрудников первой линии в выполнении задач по непрерывному мониторингу;
* повышение уровня экспертизы сотрудников центра в расследовании и реагировании на инциденты.

Далее производится совершенствование SOC для достижения определенного уровня зрелости.   
Трансформация процессов обеспечения ИБ в связи с запуском SOC   
Перед запуском SOC существующие в организации процессы обеспечения ИБ необходимо адаптировать. SOC – это прежде всего автоматизация обработки большого потока информации, выявление реальных инцидентов и оперативное реагирование на них.   
В классическом понимании к базовым процессам ИБ относятся:

* управление ИТ-активами;
* управление уязвимостями;
* управление доступом;
* криптографическая защита;
* управление инцидентами;
* защита от вредоносного ПО;
* повышение осведомленности.

Все указанные процессы в рамках создания SOC должны быть автоматизированы для оперативной обработки большого объема информации. Кроме того, для повышения уровня зрелости SOC и повышения уровня защищенности ИТ-инфраструктуры необходимо регулярное улучшение выстроенных процессов, их детальная конкретизация и план дальнейшего развития. SOC позволяет не только автоматизировать базовые процессы ИБ, но и выстроить новые, более эффективные процедуры обеспечения ИБ.

# **Перспективы**

1. Дальнейшее расширение системы в ширину(количество районов автоматизации) и в глубину(качественная проработка системы в процессе её эксплоатаци0
2. Карта внедрения -  несколько городов пробников в которых наблюдается максимальное совпадение системы с первичным шаблоном(для ускорения её построения)
3. Обмен опыта между районами автоматизации и таким образом с увеличением количественного показателя системы увеличение в математической прогрессии качественных аспектов
4. После достижения системой определённого порога в количественном и качественном аспектах возможно создание единого по стране центра автоматизации\коммутации для обеспечения наивысшего уровня взаимодействия между районами и максимально сжатого времени расширения и доработки системы

# **Социальный эффект**

**Социальное воздействие / социальный эффект (Impact)**

те благоприятные изменения, которые ожидаются от деятельности предприятия. Эти результаты проявляются, например, в изменении условий воспитания детей, здоровья клиентов, их трудоустройства или доходов

**Непосредственные результаты**

Под этим термином подразумеваются товары или услуги, которые сами по себе способствуют решению социальных проблем. Например, некая организация предлагает образовательные курсы по различным профессиям, помогающие людям переучиваться на более востребованные специальности.

Можно также посчитать количество академических часов, привлеченных преподавателей, количество специальностей, по которым происходит обучение и т.д.

**Социальные результаты**

Социальные результаты — это изменения в поведении или статусе людей, которые воспользовались данными услугами.

Это можно было бы назвать тем конкретным социальным результатом работы социального предприятия, который мы можем измерить. Изменения могут касаться отношения, поведения, знаний, улучшения психологического состояния, материального положения, статуса в обществе, межличностных отношений и т.д.

**Социальное воздействие**

социальное воздействие — это накопленный во времени положительный социальный эффект от деятельности социального предприятия.

Можно сказать и так: когда количество социальных результатов переходит в качественное изменение жизни общества (на локальном или общенациональном уровне). То есть что-то коренным образом и в лучшую сторону поменялось в жизни общества.

**Мы можем обеспечить:**

*1) Непосредственный результат*, а именно повышение квалификации специалистов главного органа управления системы и переквалификацию специалистов должностей, не вошедших в новую структур, появления ряда новых рабочих мест

*2) Социальное воздействие* в виде создания ощущения «Защищенности» у граждан (честно хз), укрепление «Доверия» к гос структурам

3) Социальные результаты автоматизации работы централизованной системы ИБ в своей основе — это сокращение рабочей нагрузки и развитее новых областей доступных и актуальных для молодых специалистов

# **Временные показатели**

## **Сроки, определённые кейсодержателем:**

До декабря 2021 года

## **В целях первичного развёртывания системы необходимо (до середины 2-го квартала 2021):**

1. Организовать команду экспертов (допустимо не полный состав) в головном центре
2. Разработать первичные планы и грубые шаблоны для будущего рекомендательного центра
3. Развернуть средства взаимодействия между подчинёнными центрами и головным
4. На базе существующих подразделений развернуть структурные элементы в соответствии с разработанными шаблонами
5. Из развернутых элементов выделить головной

## **В целях сокращения времени первичного развёртывания необходимо:**

1. Организовать максимально безболезненный переход для специалисты чьи должности не будут востребованы в новой системе на новые должности в соответствии с их квалификацией:
2. Специалисты с полностью совпадающей квалификацией подлежат прямому переводу на новые должности с их согласия
3. Специалисты с частично совпадающей квалификацией и достаточным опытом работы в сфере после подтверждения их квалификации в соответствующих органах лицензирования (постановление правительства 79) подлежат прямому назначению на новые должности с их согласия
4. Специалисты с частично совпадающей квалификации и недостаточным опытом работы в сфере (не способные пройти подтверждение квалификации) подлежат переводу на смежные должности или в другие структурные элементы системы в соответствии с их квалификацией и при их согласии
5. Специалисты чья квалификация не совпадает с требуемой, неспособные быть назначенными на смежные должности, а также отказавшиеся от перевода в другие структурные элементы системы подлежат с их согласия до\переобучению и дальнейшему приводу на соответствующие должности
6. Минимизировать глубину системы(качественный аспект) до границ допустимых значений, в целях унификации модульных решений построения системы
7. Обеспечить максимальную интеграцию с существующими отечественными решениями в соответствии со структурными решениями регионального сегмента системы

## **В целях финального развертывания всех ветвей системы и выхода на расчётную эффективность работы (до конца 4-го квартала 2021 года) необходимо:**

1. Обеспечить не менее 75% укомплектования должностными лицами всех должностей в рассматриваемом региональном сегменте системы
2. Развертывание рекомендательного центра и обеспечение его работы со всеми необходимыми элементами системы
3. Построить решений на конечных пактах с учётом основных особенностей (развитие системы в глубину)
4. Начать организованное подключение к системе всех обеспечивающих подструктур (больницы и т.д.)
5. Организовать все мероприятия необходимые для удалённой работы специалистов в системе

## **В целях сокращения времени на финальном этапе необходимо:**

1. Отладить работу экспертной команды по созданию в случае прецедентов новых модулей структурного построения системы и внесение их в пул
2. Обеспечить доработку и отладку существующих модулей
3. Создать универсальный ключь-индефикатор для конечного специалиста с целью удаленного доступа
4. Разместить средства автоматизированного управления в узловых элементах системы и в элементах, обеспечивающих подключения внешних источников от обеспечивающих подструктур

## **Таким образом, расчетное время для начала функционирования системы – лето 2021, итоговая готовность – конец 2021**

**Мероприятия**

13. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

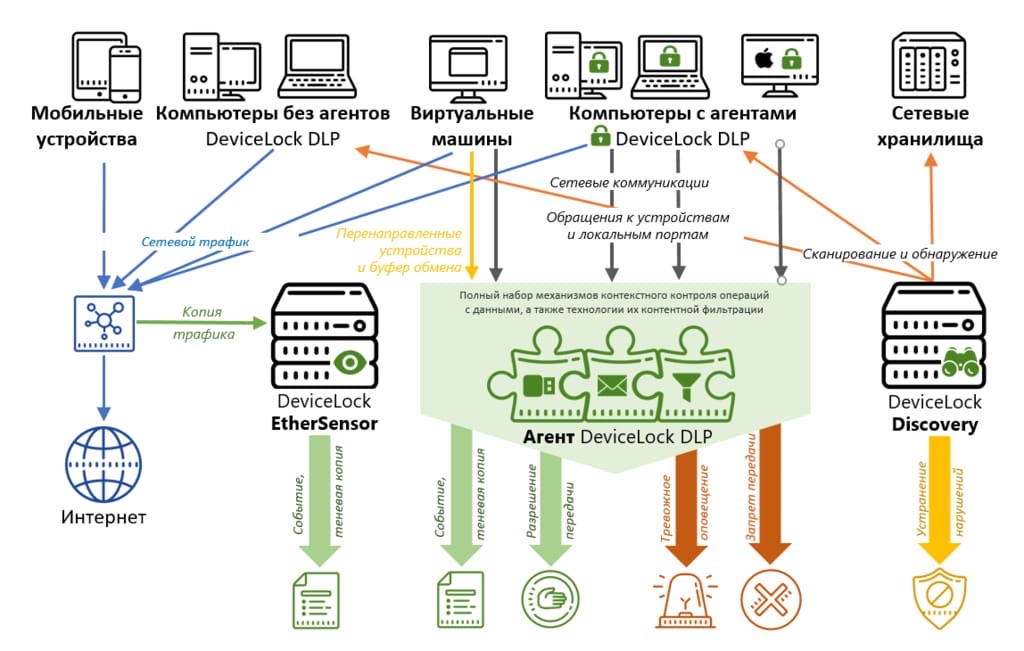
разработка системы защиты информации информационной системы;

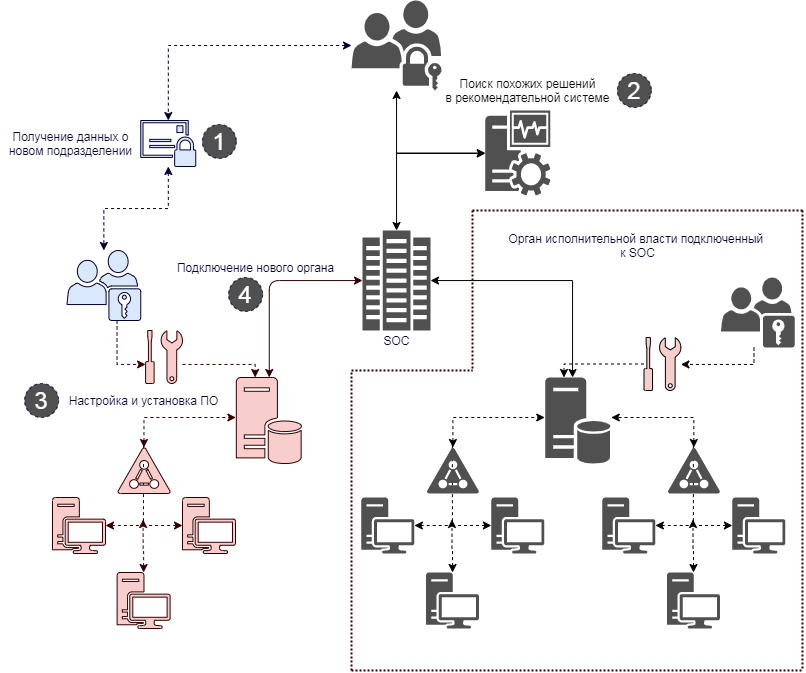
внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.





# **База НПА**

1. Конституция Российской Федерации
2. Закон РФ "О безопасности" от 05.03.1992г. № 2446-1
3. Закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 (с изм. и доп., вступающими в силу с 15.12.2007)
4. ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006г. №149-ФЗ
5. ФЗ РФ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ
6. ФЗ РФ "Электронной цифровой подписи" от 10 января 2002 г. N 1-ФЗ
7. ФЗ РФ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ
8. ФЗ РФ "О связи" 7 июля 2003 г. N 126-ФЗ
9. ФЗ "О лицензировании отдельных видов деятельности" от 8 августа 2001 года, N 128-ФЗ
10. Приказ ФСТЭК №58 от 5.02.2010г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"
11. Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
12. Указ "Об основах государственной политики в сфере информатизации" N 170 от 20.01.94г.
13. УП РФ "Вопросы Межведомственной комиссии по защите государственной тайны" от 6 октября 2004 г. № 1286
14. УП РФ "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17 марта 2008 г. N 351
15. УП РФ "Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. № 188
16. УП РФ "Вопросы федеральной службы по техническому и экспортному контролю" от 16 августа 2004 г. № 1085 (с изменениями и дополнениями от 22 марта 2005 г. № 330; от 20 июля 2005 г. №846; от 30 ноября 2006 г. № 1321)
17. УП РФ "Концепция национальной безопасности Российской Федерации" от 17 декабря 1997 г. № 1300 в редакции Указа Президента РФ от 10 января 2000 г. № 24
18. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 9.09.2000г. №Пр-1895)
19. Постановление Совета Министров — Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»
20. Постановление Правительства РФ “О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" от 15 апреля 1995 г. № 333
21. Положение о сертификации средств защиты информации Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808)
22. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"
23. Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532
24. Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
25. Постановление Правительства РФ "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15.09.2008г. №687
26. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”
27. Постановление Правительства РФ от 3 февраля 2012 г. №79 "О лицензировании деятельности по технической защите конфиденциальной информации"
28. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
29. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
30. ГОСТ 12.1.050-86 Методы измерения шума на рабочих местах
31. ГОСТ Р ИСО 7498-2-99 Государственный стандарт Российской Федерации Информационная технология взаимосвязь открытых систем базовая эталонная модель
32. ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
33. ГОСТ Р 50.1.053- 2005 Информационные технологии, основные термины и определения в области технической защиты информации
34. Приказ ФСТЭК России от 11 февраля 2013 г. N 17