апрель 2025

ПРАКТИКА КОНТРОЛЬНО-СЧЕТНОЙ ПАЛАТЫ МОСКВЫ ПО ОРГАНИЗАЦИИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Информационно-аналитическая комиссия
Совета контрольно-счетных органов
при Счетной палате Российской Федерации

Система управления информационной безопасностью в КСП Москвы (как организована информационная безопасность)

Структура управления ИБ

- Ответственное лицо за обеспечение информационной безопасности в КСП Москвы
- Ответственное лицо за организацию обработки персональных данных в КСП Москвы
- Информационно-техническая комиссия КСП Москвы
- Администратор информационной безопасности ИИКТ КСП Москвы
- Администратор ИИКТ КСП Москвы
- Уполномоченное структурное подразделение
- Работники КСП Москвы

Основные элементы системы информационной безопасности КСП Москвы

Свод организационно-распорядительных документов по обеспечению информационной безопасности и защите информации и в области обработки персональных данных

Система защиты информации Информационно-аналитической системы КСП Москвы[1] в составе инфраструктуры информационно-коммуникационных технологий КСП Москвы

Внутренние проверки состояния системы защиты информации[2] и внешние контроли защиты информации в Информационно-аналитической системе КСП Москвы[3], проверки условий обработки персональных данных[4]

[1] Информационно-аналитическая система КСП Москвы аттестована на соответствие требованиям законодательства Российской Федерации, предъявляемым к государственным информационным системам третьего класса защищенности.

[2] Предусмотрены организационно-распорядительными документами по обеспечению информационной безопасности и защите информации в КСП Москвы.

[3] Предусмотрены требованиями по поддержанию информационной системы в аттестованном состоянии.

[4] Осуществляются **в рамках внутреннего контроля** за соблюдением законодательства Российской Федерации и ЛНПА КСП Москвы в области персональных данных, в том числе требований к защите персональных данных.

Состав ОРД КСП Москвы

1. **Политика** информационной безопасности КСП Москвы.
2. **Положение** по информационной безопасности КСП Москвы (с приложениями).
3. **Модель угроз** информационной безопасности КСП Москвы.
4. **Регламент доступа** к информационным ресурсам ИИКТ КСП Москвы.

   4.1. Матрица доступа к информационным ресурсам ИИКТ КСП Москвы (ролевая модель доступа).

   4.2. Минимальный перечень информации, предусматриваемый в форме Заявки на предоставление (прекращение) доступа к ИР ИИКТ КСП Москвы.
5. **Положение об информационно-технической комиссии** КСП Москвы.
6. **Состав** информационно-технической комиссии КСП Москвы.

ОРД по обеспечению информационной безопасности и защите информации

ОРД в области обработки персональных данных

1. **Политика** обработки персональных данных КСП Москвы.
2. **Правила** обработки персональных данных.
   2.1. Журнал инструктажа.
   2.2. Журнал учета согласий.
   2.3. Форма акта об удалении ПДн**.**
3. **Правила** рассмотрения запросов субъектов ПДн.
   3.1.Форма обращения о предоставлении ПДн.
4. **Правила** осуществления внутреннего контроля
5. **Правила** работы с обезличенными ПДн.
6. **Перечень** ИСПДн.
7. **Перечень** персональных данных.
8. **Перечень** должностей, ответственных за обезличивание ПДн.
9. **Перечень** должностей, допущенных к обработке ПДн
10. **Положение** об обработке персональных данных в КСП Москвы.
11-16. **Типовые формы:**
   - **Обязательство** уполномоченного работника.
   - **Согласие** на обработку ПДн.
   - **Согласие** на распространение ПДн.
   - **Согласие** на обработку ПДн физ. лиц.
   - **Разъяснения** последствий отказа предоставления ПДн.
   - **Отзыв** согласия на обработку ПДн.
17. Порядок **доступа** в помещения.

Состав ОРД КСП Москвы (продолжение)

1. **Инструкция администратора ИИКТ** КСП Москвы.
2. **Инструкция администратора ИБ ИИКТ** КСП Москвы.

Порядок ведения журнала проведения инструктажа работников КСП Москвы по соблюдению требований ИБ.

3. **Структурная схема** ИИКТ КСП Москвы (защищаемый периметр).
4. Адаптированный **базовый перечень мер защиты** информации в ИИКТ КСП Москвы.
5. Инструкция по **парольной** защите в ИИКТ КСП Москвы.
6. Инструкция **пользователя** по обеспечению безопасности информации при работе в ИИКТ КСП Москвы.
7. Инструкция по работе должностных лиц КСП Москвы с информацией при проведении контрольных мероприятий **в проверяемых организациях**.
8. Перечень **разрешенного** к использованию программного обеспечения.
9. Порядок резервирования и **восстановления** работоспособности технических средств и программного обеспечения, баз данных и СЗИ в ИИКТ КСП Москвы.
10. Перечень **уполномоченных** должностных лиц, наделенных правом доступа к техническим средствам ИИКТ Москвы (в пределах контролируемой зоны).
11. Форма **заявки** о событии ИБ для размещения в электронном виде на Портале информационно-аналитической системы КСП Москвы.
12. Программа **проведения проверок** состояния системы защиты информации.
13. Регламент внесения **изменений в конфигурацию** Информационно-аналитической системы КСП Москвы.
14. Порядок предоставления пользователям КСП Москвы доступа к информационно-телекоммуникационной сети **Интернет**.
15. Порядок предоставления работникам КСП Москвы доступа к системе **корпоративной** электронной почты.

Положение по информационной безопасности КСП Москвы

Из Положения об информационно-технической комиссии КСП Москвы

1. Комиссия вырабатывает предложения по:
- определению **объектов критической информационной инфраструктуры** и категорий значимости объектов критической информационной инфраструктуры КСП Москвы;
- рассмотрению **причин, последствий и результатов ликвидации** последствий высокоопасных и опасных инцидентов информационной безопасности в ИИКТ КСП Москвы;
- проведению **плановых внутренних проверок** защиты информации в ИИКТ КСП Москвы и аудита информационной безопасности внешними организациями;
- результатам **оценки внутренних проверок** защиты информации и внешнего аудита информационной безопасности в ИИКТ КСП Москвы;
- результатам **оценки выполнения мероприятий** Плана информационно-технологического обеспечения КСП Москвы (далее - План ИТО), развитию инфраструктуры информационно-коммуникационных технологий и цифровых сервисов КСП Москвы;
- актуализации локальных нормативных правовых актов (далее - ЛНПА) КСП Москвы по **вопросам обеспечения информационной безопасности и защите информации**;
- развитию, внедрению и использованию информационных технологий и информационных ресурсов в основной деятельности КСП Москвы;
- разработке технических заданий и иной основополагающей документации в сфере информационных технологий, цифровизации и цифровой трансформации КСП Москвы;
- иным вопросам, обусловленным требованиями федерального законодательства.

2. Комиссия в своей деятельности осуществляет подготовку предложений по актуализации:
- **Концепции развития** инфраструктуры информационно-коммуникационных технологий и цифровых сервисов КСП Москвы (далее - Концепция);
- **Плана ИТО** с учетом приоритетов и достигнутых результатов реализации Концепции;
- перечня правовых, организационных и технических **мер** по обеспечению информационной безопасности и защите информации;
- ЛНПА КСП Москвы, регламентирующих (определяющих): **порядок проверки** уровня защищенности информации в ИИКТ КСП Москвы, систему оценки рисков информационной безопасности, модель угроз информационной безопасности;
- иным вопросам, обусловленным требованиями федерального законодательства.

Полномочия ИТК КСП Москвы

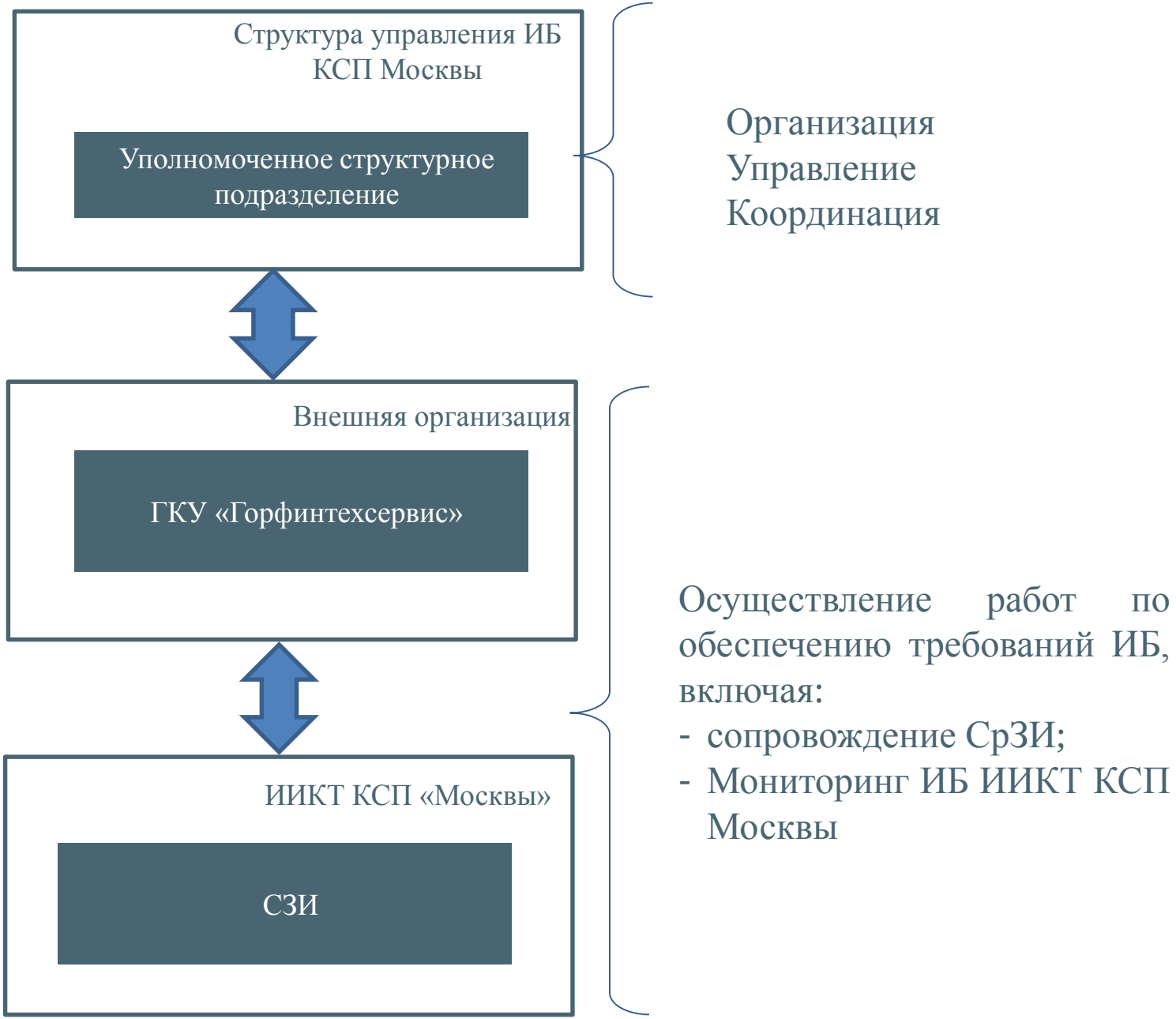
Из Положения об информационно-технической комиссии КСП Москвы (продолжение)

3. Комиссия **рассматривает результаты контроля** за:
- **соблюдением требований** Регламента доступа к информационным ресурсам ИИКТ КСП Москвы;
- обеспечением установленного требованиями ЛНПА **уровня защищенности** информации в ИИКТ КСП Москвы, в том числе на основании результатов **мониторинга** уровня защищенности ИИКТ КСП Москвы (внутренний контроль) и материалам аудита информационной безопасности (внешний контроль).

2.4. Комиссия **осуществляет контроль** за:
- **выполнением** мероприятий по обеспечению информационной безопасности и защите информации;
- **результативностью** мер по ликвидации последствий высокоопасных и опасных инцидентов информационной безопасности в ИИКТ КСП Москвы;
- **исполнением** решений, принятых на заседаниях Комиссии.

Полномочия ИТК КСП Москвы

Кем организована и кто оказывает помощь в поддержке ИБ



Основные проблемы обеспечения ИБ и их решения

Повышение культуры киберосведомленности работников

Ежегодно перед праздниками число фишинговых атак растет на 20-30%

Анонимы в мессенджерах, установив на аватар фото руководителей взятых из публичных источников, пытаются ввести в заблуждение работников

Методы социальной инженерии злоумышленников становятся всё более изощренными и настойчивыми

Решения

Организовать непрерывный **процесс обучения и информирования работников** о различных аспектах информационной безопасности, угрозах и методах их предотвращения

Проведение инструктажей. Оперативное оповещение об актуальных тактиках и сценариях злоумышленников (объявление на внутреннем портале, рассылка на email). Отказ от общения по рабочим вопросам в мессенджерах

Discord, Snapchat, Skype, Microsoft Teams, Threema, Viber, WhatsApp, WeChat, Telegram. Функционал указанных приложений подпадает под запреты ч. 8 ст. 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее – Закон № 149-ФЗ).
Указанная норма вступила в силу с 1 марта 2023 года. Ранее Роскомнадзор публиковал перечень мессенджеров, которые могут быть отнесены к сервисам, нежелательным к использованию в работе организаций (операторов), указанных в ч. 8 ст. 10 Закона № 149-ФЗ

Сопровождение СЗИ

Переобучение персонала на работу с отечественными СРЗИ

Затраты на продление технической поддержки СРЗИ и обновление баз сигнатур

Несовместимость версий пакетов СРЗИ после выхода обновлений отечественных ОС

Планировать работы по сопровождению СЗИ:
- замена элементов инфраструктуры на отечественные решения;
- обучение работе с отечественными ОС, ПО, СРЗИ;
- мониторинг наличия и сроков действия сертификатов у СРЗИ;
- планировать порядка 40% первоначальной стоимости СРЗИ на продление технической поддержки ежегодно;
- сопоставление доступных обновлений формулярам используемого СРЗИ. Консультации с технической поддержкой до обновления

Обеспечение ИБ официального сайта



- ЦОД, имеющий сертификат класса защищенности не ниже класса защищенности, присвоенного информационной системе официального сайта;
- ЦОД, имеющий класс отказоустойчивости Tier II или Tier III;
- отечественное ПО сайта (система управления сайтом), имеющее актуальную техническую поддержку;
- организованная СТП официального сайта;
- услуга «защита от DDOS»;

Направления совершенствования работы ИБ КСП Москвы

1.°Должностные лица, ответственные за организацию обработки персональных данных и за обеспечение безопасности персональных данных **не реже одного раза в пять лет** должны проходить повышение квалификации по программам «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных», «Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну».

2. Security Awareness - процесс обучения и информирования работников о различных аспектах информационной безопасности, угрозах и методах их предотвращения.

3. Совершенствование процессов, обеспечивающих поддержание системы в аттестованном состоянии.

Из практики обработки ПДн. На примере протоколов об административных правонарушениях, составляемых в рамках контрольных мероприятий

