



САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ  
**«ПЕТЕРБУРГСКИЙ МЕТРОПОЛИТЕН»**

УТВЕРЖДАЮ  
Главный инженер – первый заместитель  
начальника метрополитена

\_\_\_\_\_ А.В. Спиркин

«26» \_\_\_\_\_ 2025 г.

**ПОЛОЖЕНИЕ**  
**о порядке организации и управления защитой информации**  
**в ГУП «Петербургский метрополитен»**

## СОДЕРЖАНИЕ

1. Перечень используемых сокращений и терминов	3
2. Общие положения	7
3. Порядок организации и управления защитой информации	8
4. Организация и управление защитой информации в создаваемых информационных (автоматизированных) системах	11
5. Организация и управление защитой информации в информационных (автоматизированных) системах и сетях, принятых в эксплуатацию	16
6. Обязанности и права должностных лиц, осуществляющих мероприятия по информационной безопасности	28
7. Взаимодействие по вопросам защиты информации	30
ПРИЛОЖЕНИЕ:	
1. Перечень централизованных мер защиты информации	32
2. Перечень компенсирующих мер защиты информации	33
3. Перечень нормативных правовых актов и методических документов по защите информации	35

## 1. Перечень используемых сокращений и терминов

**АС** – автоматизированная система.

**ЗО** – значимый объект.

**ИС** – информационная система.

**ИСПДн** – информационная система персональных данных.

**КИИ** – критическая информационная инфраструктура.

**НСД** – несанкционированный доступ.

**МНИ** – машинный носитель информации.

**ОС** – операционная система.

**ПО** – программное обеспечение.

**САВЗ** – средство антивирусной защиты.

**СВТ** – средство вычислительной техники.

**СБ** – система безопасности.

**СЗИ** – система защиты информации.

**СрЗИ** – средство защиты информации.

**СКЗИ** – средство криптографической защиты информации.

**ТЗИ** – техническая защита информации.

**УБИ** – угрозы безопасности информации.

**ЦБ** – центр управления информационной безопасностью Управления метрополитена.

**Автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Информационная система (ИС)** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационно-телекоммуникационная (информационная) инфраструктура** – совокупность информационных (автоматизированных) систем, информационно-телекоммуникационных сетей, сайтов в сети Интернет, отдельных средств вычислительной техники, программного обеспечения, обеспечивающих систем, используемых оператором для реализации функций (полномочий) или видов деятельности.

**Защита информации** – деятельность, направленная на предотвращение утечки

защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Политика безопасности (информации в организации)** – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

**Система защиты информации автоматизированной системы** – совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

**Техническая защита информации (ТЗИ)** – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

**Защита информации от несанкционированного доступа (ЗИ от НСД)** – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

**Защита информации от утечки** – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

**Защищаемое помещение** – помещение (служебный кабинет, конференц-зал и т.д.), специально предназначенное для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

**Инцидент информационной безопасности** – одно или несколько нежелательных, или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности (ГОСТ Р ИСО/МЭК 27000-2021).

**Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

**Критическая информационная инфраструктура** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Значимый объект критической информационной инфраструктуры** – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

**Модель угроз (безопасности информации)** – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

**Событие информационной безопасности** – выявленное наступление состояния системы, сервисов или вычислительной сети, указывающее на возможное нарушение политики информационной безопасности, на сбой или отсутствие необходимых мер защиты или на прежде неизвестную ситуацию, относящейся к обеспечению безопасности.

**Безопасность информации** – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

**Мониторинг безопасности информации** – постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

**Аудиторская проверка информационной безопасности в организации** – аудит информационной безопасности: периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

**Объект защиты информации** – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены.

**Объекты критической информационной инфраструктуры**

– информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Средства вычислительной техники (СВТ)** – совокупность элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Угроза (безопасности информации)** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

**Утечка информации** – неконтролируемое распространение защищаемой информации в результате ее разглашения или несанкционированного доступа к ней.

**Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Эффективность защиты информации** – степень соответствия результатов защиты информации цели защиты информации.

**Требование по защите информации** – установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

## 2. Общие положения

2.1. Организация и управление защитой информации в ГУП «Петербургский метрополитен» (далее – метрополитен) определяются законодательством Российской Федерации, актами Президента Российской Федерации и актами Правительства Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, государственными стандартами по защите информации, локальными нормативными актами метрополитена, в том числе настоящим «Положением о порядке организации и управления защитой информации в ГУП «Петербургский метрополитен».

2.2. Целью организации и управления защитой информации является исключение или существенное снижение негативных последствий (ущерба) в отношении метрополитена вследствие нарушения функционирования ИС (АС, сети) метрополитена в результате реализации УБИ.

2.3. Основные задачи, руководящие принципы, правила и процедуры организации и управления защитой информации изложены в действующих Концепции информационной безопасности и Политике информационной безопасности метрополитена.

2.4. Настоящее «Положение о порядке организации и управления защитой информации в ГУП «Петербургский метрополитен» (далее – Положение) является основным документом по организации информационной безопасности в ИС (АС, сетях) и на объектах информатизации метрополитена. Настоящее Положение применяется для организации защиты (некриптографическими методами) информации, предотвращения несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, блокирования доступа к информации, содержащейся в ИС (АС, сетях) и обеспечения безопасности объектов КИИ метрополитена.

2.5. Организация защиты конфиденциальной информации, представленной на бумажных носителях и других материальных носителях информации, определена в действующей Инструкции о порядке работы с конфиденциальной информацией в ГУП «Петербургский метрополитен».

2.6. Настоящее Положение не распространяется на организацию защиты сведений, составляющих государственную тайну, организацию защиты речевой конфиденциальной информации в защищаемых помещениях и предотвращение утечки защищаемой информации по техническим каналам.

2.7. Требования настоящего Положения являются обязательными для исполнения работниками подразделений, ответственных за обеспечение информационной безопасности, а также подразделений, эксплуатирующих и (или) обеспечивающих функционирование (сопровождение, обслуживание, ремонт) ИС (АС, сетей) метрополитена.

2.8. Настоящее Положение разработано в соответствии с нормативно-правовыми актами Российской Федерации по вопросам защиты информации и нормативно-методическими документами Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК РФ), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор России) Министерства цифрового развития, связи и массовых коммуникаций (Минцифры России) (далее – Регуляторы).

2.9. В настоящем Положении используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации и национальными стандартами в области защиты информации.

### **3. Порядок организации и управления защитой информации**

3.1. Система организации и управления защитой информации предусматривает реализацию правовых, организационных, технических и иных мер, направленных на обеспечение информационной безопасности (защиты информации) ИС (АС, сетей) метрополитена.

3.2. Для создаваемой ИС (АС, сети) должно быть определено подразделение – заказчик, для ИС (АС, сети), принятой в эксплуатацию, должно быть определено подразделение – владелец.

3.3. Управление защитой информации в метрополитене должно осуществляться с учетом действующей Политики информационной безопасности и включать следующие процессы:

I. Планирование мероприятий по организации и управлению защитой информации.

II. Обеспечение организации и управления защитой информации в ИС (АС, сетях) на этапах создания и эксплуатации.

III. Контроль состояния организации и управления защитой информации в метрополитене и оценка состояния защиты информации.

IV. Совершенствование организации и управления защитой информации.

3.4. Планирование организации и управления защитой информации включает разработку и утверждение ежегодного Плана мероприятий по совершенствованию защиты информации, содержащейся в ИС (АС, сетях) (далее – План мероприятий), в котором должны быть указаны конкретные задачи в рамках организации и управления защитой информации.

3.4.1. План мероприятий разрабатывается ЦБ и утверждается заместителем начальника метрополитена, ответственным за обеспечение защиты информации в метрополитене и доводится до подразделений (работников) в касающейся их части.

3.4.2. План мероприятий может по решению руководства разрабатываться на более длительный срок с учетом имеющихся планов по управлению защитой информации в метрополитене или СЗИ ИС (АС, сети).

3.4.3. План мероприятий должен содержать наименования мероприятий по организации и управлению защитой информации, сроки их выполнения, сведения о подразделениях (работниках), ответственных за реализацию каждого мероприятия, а также сведения о работниках ЦБ, ответственных за контроль выполнения каждого мероприятия.

3.4.4. Планирование мероприятий по обеспечению безопасности ЗО КИИ осуществляется с участием подразделений, эксплуатирующих и/или обеспечивающих функционирование ЗО КИИ. Указанные мероприятия включаются в общий план мероприятий по защите информации отдельным разделом или оформляются в виде отдельного плана.

3.4.5. На основании нормативно-методических документов Регуляторов (24, 26.5), приведенных в приложении № 3 к настоящему Положению, ЦБ подготавливаются планы мероприятий по реагированию на целевые компьютерные атаки при установлении уровней опасности на объектах КИИ.

3.4.6. По отдельным направлениям работ по обеспечению информационной безопасности при необходимости подготавливаются частные планы мероприятий: план администрирования безопасности, план обучения работников, план тренировок, план закупок работ, услуг и средств защиты информации и т.п.

3.5. Организация и управление защитой информации в метрополитене должна включать проведение следующих мероприятий:

- разработка и актуализация внутренних стандартов и регламентов по защите информации;
- реализация централизованных технических мер защиты информации в отношении ИС (АС, сети);
- проведение обучения и инструктажей работников по информационной безопасности;

– оценка состояния защиты информации.

3.5.1. Разрабатываемые внутренние стандарты и регламенты по защите информации должны устанавливать требования к реализации мер по защите информации и содержать порядок проведения мероприятий или описание реализуемых процессов по защите информации.

3.5.2. Разработку внутренних стандартов и регламентов по защите информации организует ЦБ.

3.5.3. В централизованные технические меры защиты информации включаются меры, которые могут быть реализованы на уровне всей информационной инфраструктуры метрополитена и могут действовать в отношении ИС (АС) систем. Перечень централизованных технических мер защиты информации приведен в приложении № 1 к настоящему Положению.

3.5.4. За реализацию централизованных технических мер защиты информации несет ответственность ЦБ.

3.5.5. Информирование и обучение работников – пользователей ИС (АС) по вопросам информационной безопасности должно включать:

- а) доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;
- б) проведение лекций, семинаров, обучающих игр по вопросам защиты информации;
- в) проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;
- г) проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

3.5.6. Доведение до пользователей информационных материалов, проведение тренировок по вопросам информационной безопасности организует и обеспечивает ЦБ.

3.5.7. Доведение до работников требований по защите информации при приеме на работу, обучение работников на специальных курсах во внешних организациях, организуется при участии Службы управления персоналом Управления метрополитена.

3.5.8. Доведение до работников требований нормативно-правовых актов и распорядительных документов по обеспечению информационной безопасности организует руководство подразделений метрополитена.

3.6. Оценка состояния защиты информации должна осуществляться

3.6. Оценка состояния защиты информации должна осуществляться на основании нормативно-методических документов Регуляторов. Оценка проводится на основе показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации и показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации.

3.7. Расчет и оценка показателя защищенности должны проводиться не реже одного раза в шесть месяцев, расчет и оценка показателя уровня зрелости должны проводиться не реже одного раза в два года.

3.8. Периодический контроль за состоянием защищенности и оценка состояния защиты информации проводится ЦБ, внешний аудит проводится с привлечением сторонней организации, имеющей соответствующую лицензию на осуществление деятельности в области технической защиты конфиденциальной информации.

#### **4. Организация и управление защитой информации в создаваемых информационных (автоматизированных) системах**

4.1 Мероприятия по защите информации являются составной частью работ по созданию и эксплуатации ИС (АС, сетей) метрополитена и обеспечиваются на всех стадиях жизненного цикла (этапах) создания (внедрения, модернизации), в ходе эксплуатации и вывода из эксплуатации создаваемой ИС (АС, сети).

4.2 Мероприятия по защите информации в создаваемой ИС (АС, сетей) организует подразделение-заказчик или подразделение-владелец ИС (АС, сети) с привлечением ЦБ.

4.3 В целях защиты информации в создаваемых ИС (АС, сетях) должны быть проведены следующие мероприятия:

- 1) Формирование требований к защите информации в ИС (АС, сети);
- 2) Разработка системы защиты информации (СЗПДн, СБ ЗОО КИИ);
- 3) Внедрение системы защиты информации (СЗПДн, СБ ЗО КИИ);
- 4) Оценка соответствия ИС (АС, сети) требованиям защиты информации и ввод ее в действие.

Примерное содержание мероприятий в части создания системы защиты информации приведено в национальном стандарте ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

4.4 Формирование требований к защите информации включает проведение следующих мероприятий:

- принятие решения о необходимости защиты информации, содержащейся в ИС (АС, сети);
- классификацию ИС (АС, сети) по требованиям защиты информации;
- оценку УБИ, разработку модели угроз безопасности информации (при необходимости);
- определение требований к СЗИ.

4.5 Принятие решения о необходимости создания СЗИ осуществляют подразделение – заказчик или владелец ИС (АС, сети) при участии ЦБ. Принятое решение должно включать определение целей и задач защиты информации, основных этапов создания СЗИ и функций участников по обеспечению защиты информации.

4.6 Класс защищенности ИС (АС, сети) (категория значимости объекта КИИ или уровень защищенности персональных данных в ИСПДн) определяется комиссией, назначенной приказом начальника метрополитена. Результаты классификации (категорирования объекта КИИ, определения уровня защищенности персональных данных) оформляются Актом.

Порядок определения класса защищенности ИС (АС, сети), категории значимости объекта КИИ и порядок действий комиссий определены в нормативно-правовых актах Регуляторов (13), (14) и (16), приведенных в приложении № 3 к настоящему Положению.

4.7 Оценка УБИ должна проводиться в соответствии с действующей методикой, утвержденной ФСТЭК РФ ((21) приложение № 3 к настоящему Положению).

4.7.1. В качестве исходных данных для определения УБИ должен использоваться банк данных угроз безопасности информации (bdu.fstec.ru) ФСТЭК России, оценка УБИ должна проводиться на основании данных о возможностях (потенциале) внешних и внутренних нарушителей, возможных уязвимостях ИС (АС, сети), способах реализации и последствиях от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

4.7.2. Для определения УБИ владелец ИС (АС, сети) совместно с подразделением, которое будет обеспечивать ее функционирование, должен подготовить и предоставить в ЦБ следующие исходные данные:

- сведения о структуре ИС (АС, сети), составе программного обеспечения и аппаратных средств;
- сведения о физических, логических, функциональных и технологических взаимосвязях между сегментами ИС (АС, сети) и с иными ИС и информационно-телекоммуникационными сетями;

- режимы обработки информации в ИС (АС, сети) и в ее отдельных сегментах;
- применяемые информационные технологии и особенности функционирования;
- сведения о бизнес-процессах, деятельность которых обеспечивает ИС (АС, сеть);
- сведения о финансовой ценности, возможном ущербе в случае нарушения/прекращения функционирования ИС (АС, сети) и иные данные, необходимые для оценки рисков.

4.7.3. К разработке Модели УБИ должны привлекаться организации, имеющие лицензию ФСТЭК РФ на осуществление деятельности по технической защите конфиденциальной информации.

4.8. Требования к СЗИ должны быть определены с учетом класса защищенности (категории значимости объекта КИИ, уровня защищенности персональных данных) ИС (АС, сети) и перечня актуальных УБИ. Содержание требований должно быть включено в раздел «Требования к защите информации от несанкционированного доступа» Технического задания на создание (модернизацию) ИС (АС, сети).

4.9. Для ИС (АС, сети), создаваемой на базе действующей системы, разрабатывается Техническое задание на создание СЗИ или дополнение к основному Техническому заданию на ИС (АС, сеть), в которое включают требования к СЗИ. Указанные требования подлежат согласованию с ЦБ.

4.10. К разработке СЗИ должны привлекаться организации, имеющие лицензию ФСТЭК РФ на осуществление деятельности по технической защите конфиденциальной информации.

4.11. В проектной документации на СЗИ ИС (АС, сети) разработчиком проекта должны быть определены и указаны:

- типы субъектов доступа и объектов доступа;
- методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа на основе списков, меток безопасности, ролей и иных правил;
- меры защиты информации, подлежащие реализации в СЗИ;
- виды, типы и стоимость СрЗИ, обеспечивающие реализацию технических мер защиты информации, с учетом их совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств, а также класса защищенности ИС (АС, сети);

- структура системы защиты информации, включая состав (количество) и места размещения ее элементов;
- параметры настройки ПО, включая программное обеспечение СрЗИ, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС (АС, сети), приводящих к возникновению УБИ;
- меры защиты информации при взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

4.12. Эксплуатационная документация на СЗИ ИС (АС, сети) должна включать:

- описание структуры СЗИ;
- описание состава, мест установки, параметров и порядка настройки СрЗИ, ПО и технических средств;
- описание правил эксплуатации СЗИ.

4.13. Макетирование и тестирование СЗИ ИС (АС, сети) (проводятся при необходимости) включает:

- проверку работоспособности и совместимости выбранных СрЗИ с информационными технологиями и техническими средствами;
- проверку выполнения выбранными СрЗИ требований к СЗИ;
- корректировку проектных решений, разработанных при создании.

4.14. На стадии внедрения СЗИ ИС (АС, сети) должны быть проведены следующие мероприятия:

- установка и настройка СрЗИ в ИС (АС, сети);
- разработка документов, определяющих правила и процедуры обеспечения защиты информации (стандартов, регламентов по защите информации);
- внедрение организационных мер защиты информации;
- предварительные испытания СЗИ (при необходимости);
- опытная эксплуатация СЗИ (при необходимости);
- анализ уязвимостей ИС (АС, сети) и принятие мер защиты информации по их устранению;
- приемочные испытания СЗИ (при необходимости).

4.15. Установка и настройка СрЗИ должна организовываться подразделением, обеспечивающим функционирование ИС (АС, сети) при участии организации – лицензиата по ТЗИ, в соответствии с эксплуатационной документацией на систему и СрЗИ.

4.16. Внедрение организационных мер защиты информации должно включать:

- реализацию правил разграничения доступа субъектов доступа к объектам

доступа, введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и ПО;

- проверку полноты описания в внутренних стандартах и регламентах по защите информации действий работников по реализации организационных мер защиты информации;

- отработку действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

4.17. Предварительные испытания, опытная эксплуатация и приемочные испытания СЗИ включают проверки выполнения требований, работоспособности, готовности пользователей и администраторов к эксплуатации СЗИ.

4.18. Анализ уязвимостей ИС (АС, сети) проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации УБИ и должен включать: проверку отсутствия известных уязвимостей ПО, технических средств и СрЗИ, правильности их установки и настройки, а также корректности работы СрЗИ при их взаимодействии с техническими средствами и ПО.

4.19. Оценка соответствия создаваемой ИС (АС, сети) нормативным требованиям по защите информации должна проводиться с учетом действующего Порядка организации и проведения работ по аттестации, утвержденного ФСТЭК РФ, по согласованной с подразделением-заказчиком программе и методике. К проведению оценки могут привлекаться на договорной основе юридические лица (индивидуальные предприниматели), имеющие лицензию ФСТЭК РФ на осуществление деятельности по технической защите конфиденциальной информации.

4.20. Подразделение – заказчик создаваемой ИС (АС, сети) должно организовать:

- подготовку технического задания на создание ИС (АС, сети), содержащего раздел Требования по защите информации от несанкционированного доступа;

- планирование расходов на услуги по защите информации в создаваемой ИС (АС, сети), в том числе: по моделированию УБИ, проектированию СЗИ, расходов на установку и настройку СрЗИ, испытания СЗИ (при необходимости) и оценку соответствия создаваемой ИС (АС, сети) требованиям безопасности;

- планирование расходов на закупку СрЗИ в соответствии с техническим проектом на СЗИ.

4.21. ЦБ на этапе создания (модернизации) СЗИ ИС (АС, сети) метрополитена должен обеспечивать:

- методическое руководство и контроль при выборе мер защиты

информации, подлежащих реализации;

- методическое руководство и контроль при определении СрЗИ, обеспечивающих реализацию технических мер защиты информации;
- контроль состава и содержания проектной, эксплуатационной документации на СЗИ;
- актуализацию внутренних стандартов и регламентов по защите информации;
- контроль внедрения организационных мер защиты информации.

## **5. Организация и управление защитой информации в информационных (автоматизированных) системах и сетях, принятых в эксплуатацию**

5.1. Мероприятия по защите информации ИС (АС, сети) принятой в эксплуатацию, должны осуществляться в соответствии с действующими нормативными документами Регуляторов, эксплуатационной документацией на систему защиты информации, внутренними стандартами и регламентами по защите информации.

5.2. Мероприятия по защите информации в ИС (АС, сети), принятых в эксплуатацию, организует подразделение – владелец ИС (АС, сети). Реализуют мероприятия по защите ЦБ и подразделение, которое обеспечивает функционирование (сопровождение) ИС (АС, сети).

При необходимости к мероприятиям по защите информации в ИС (АС, сети) подразделением – владельцем в соответствии с законодательством Российской Федерации привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

5.3. В ИС (АС, сети), принятых в эксплуатацию, должны проводиться следующие мероприятия:

- выявление и оценка УБИ;
- контроль конфигураций ИС (АС, сетей);
- управление уязвимостями;
- управление обновлениями;
- обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;
- обеспечение защиты информации при применении конечных устройств;
- обеспечение защиты информации при применении мобильных устройств;
- обеспечение защиты информации при удаленном доступе пользователей;

- обеспечение защиты информации при беспроводном доступе пользователей;
- обеспечение защиты информации при предоставлении пользователям доступа к ИС (АС), предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных (далее – привилегированный доступ);
  - обеспечение мониторинга информационной безопасности;
  - обеспечение разработки безопасного ПО;
  - обеспечение физической защиты ИС (АС, сетей);
  - обеспечение непрерывности функционирования ИС (АС, сетей) при возникновении нештатных ситуаций;
  - повышение уровня знаний и информированности пользователей по вопросам защиты информации;
  - обеспечение защиты информации при взаимодействии с подрядными организациями;
  - обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;
  - обеспечение защиты информации при использовании искусственного интеллекта;
  - реализация в ИС (АС, сетях) мер по их защите и защите содержащейся в них информации;
  - проведение контроля уровня защищенности информации;
  - обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5.4. Периодичность проведения мероприятий, указанных в пункте 5.3 настоящего Положения, должна быть определена в Плане мероприятий.

5.5. Мероприятия по выявлению и оценке УБИ в действующих ИС (АС, сетях) организует ЦБ, который организует поиск актуальных угроз, их приоритезацию, оповещение подразделений о выявленных актуальных угрозах и принятие мер по их блокированию (нейтрализации). Решение о необходимости разработки модели УБИ принимается ответственным лицом.

5.6. Мероприятия по контролю конфигураций ИС (АС, сетей) должны исключать несанкционированное изменение состава программных, программно-аппаратных средств, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечивать обнаружение фактов несанкционированных изменений и выявление причин изменений.

5.7. Контроль конфигураций ИС (АС, сетей) должен осуществляться

на основе анализа результатов учета ИТ-активов и (или) сведений, содержащихся в автоматизированных системах хранения и управления данными. ЦБ должен быть обеспечен доступ к указанным сведениям.

5.8. Мероприятия по управлению уязвимостями должны включать выявление уязвимостей ИС (АС, сетей), оценку их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

5.9. Устранение уязвимостей, которые могут быть использованы нарушителями, или исключение возможности их использования за счет применения компенсирующих мер должно проводиться:

- в отношении уязвимостей критического уровня опасности – в срок не более 24 часов;
- в отношении уязвимостей высокого уровня опасности – в срок не более 7 календарных дней.

В отношении уязвимостей среднего и низкого уровней опасности сроки и порядок их устранения определяются во внутреннем регламенте по защите информации исходя из особенностей функционирования ИС (АС, сети).

5.10. Мероприятия по управлению обновлениями должны включать проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестирование обновлений до их применения, выдачу разрешения подразделениям на применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации с использованием безопасных настроек и конфигураций, установленных во внутренних стандартах по защите информации. Бесконтрольная установка обновлений программных, программно-аппаратных средств не допускается.

– Мероприятия по защите информации при обработке, хранении и обращении с информацией ограниченного доступа должны исключать: неправомерное распространение информации ограниченного доступа вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети Интернет; доступ к информации ограниченного доступа лиц, для которых информация не предназначена и (или) для которых такой доступ запрещен.

5.11. Мероприятия по защите информации ограниченного доступа должны включать: определение информации ограниченного доступа, определение программно-аппаратных средств, предназначенных для ее хранения, а также контроль и регистрацию всех фактов доступа пользователей к программно-аппаратным средствам, в которых хранится информация

ограниченного доступа.

5.12. Мероприятия по обеспечению защиты информации при применении конечных устройств должны исключать возможность несанкционированного доступа к ИС (АС, сетям) и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью Интернет и (или) доступные из сети Интернет. Защита конечных устройств должна включать реализацию в них мер по защите информации от несанкционированного доступа и проведении на них мониторинга и анализа процессов и событий с целью выявления актуальных угроз, а также предупреждения о произошедших событиях безопасности.

5.13. Мероприятия по обеспечению защиты информации при применении мобильных устройств должны исключить возможность несанкционированного доступа (воздействия) к ИС (АС, сетям) и содержащейся в них информации, а также к взаимодействующим с ними мобильным устройствам через каналы передачи мобильных данных, мобильные сервисы, интерфейсы и порты мобильных устройств.

5.14. При применении пользователями мобильных устройств для доступа к ИС и содержащейся в них информации в целях выполнения должностных обязанностей должны приниматься следующие меры по защите, в том числе:

- обеспечение защиты каналов передачи данных;
- осуществление доступа пользователей с применением строгой аутентификации;
- пользователем должен быть исключен несанкционированный доступ к мобильному устройству.

5.15. Применение пользователями личных мобильных устройств для доступа к ИС (АС, сетям) и содержащейся в них информации с целью выполнения своих обязанностей допускается в случае соответствия мобильных устройств требованиям безопасности и наличия возможности контроля использования мобильных устройств. Контроль использования мобильных устройств должен осуществляться в соответствии с внутренним стандартом и регламентом по защите информации.

5.16. Мероприятий по обеспечению защиты информации при удаленном доступе пользователей должны исключать возможность несанкционированного доступа (воздействия) к ИС (АС, сетям) через каналы передачи данных, интерфейсы и порты удаленно подключаемых программно-аппаратных средств. Должны приниматься меры по защите ИС (АС, сетей), обеспечиваться защита каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется удаленный доступ, исключаться несанкционированный доступ к удаленно подключаемому программно-аппаратному средству пользователя.

5.17. Удаленный доступ пользователей в целях выполнения своих

обязанностей (функций) должен осуществляться с использованием программно- аппаратных средств, выделенных предприятием и соответствующих требованиям безопасности. По согласованию с ЦБ допускается предоставление удаленного доступа с использованием личных программно-аппаратных средств пользователя при условии применения сертифицированных средств обеспечения безопасной дистанционной работы, САВЗ и иных СрЗИ, исключаяющих УБИ, связанные с удаленным доступом.

5.18. Удаленный доступ пользователей в целях выполнения своих обязанностей должен осуществляться с использованием сетей связи, расположенных на территории Российской Федерации, посредством применения средств защиты канала передачи данных, и строгой аутентификации пользователей.

5.19. Мероприятия по обеспечению защиты информации при беспроводном доступе пользователей должны исключать возможность несанкционированного доступа (воздействия) за счет несанкционированного подключения к точкам беспроводного доступа и доступа к беспроводным каналам передачи данных, подмены взаимодействующих с ними программно-аппаратных средств или доступа к ним.

5.20. При беспроводном доступе пользователей в целях выполнения своих обязанностей должны приниматься меры по защите, обеспечиваться защита беспроводных каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется беспроводной доступ. Посредством формирования конфигурации и настроек, уровней сигналов точек беспроводного доступа, используемых для подключения пользователей, должна быть исключена возможность подключения к ним лиц, не имеющих прав доступа. Указанные точки беспроводного доступа должны быть однозначно идентифицированы, а также определены места их размещения.

5.21. Точки беспроводного доступа и построенные на их основе беспроводные сети связи, используемые для доступа пользователей к ИС (АС, сетям) и содержащейся в них информации в целях выполнения ими своих обязанностей, должны быть изолированы от беспроводных сетей связи, предназначенных для доступа к сети Интернет и (или) общедоступной информации.

5.22. Мероприятия по обеспечению защиты информации при предоставлении привилегированного доступа должны исключить возможность получения привилегированного доступа лицами, для которых такой доступ запрещен, а также возможность использования повышенных прав доступа с нарушением внутренних стандартов и регламентов по защите информации. Привилегированные учетные записи должны иметь права доступа, минимально необходимые для выполнения

пользователями возложенных на них обязанностей, в соответствии с принятыми моделями доступа. Привилегированные учетные записи, имеющие права по созданию других привилегированных учетных записей, должны быть персонифицированными.

5.23. Привилегированный доступ должен осуществляться с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации - с использованием усиленной многофакторной аутентификации. Не допускается объединение в рамках одной привилегированной учетной записи или одной группы привилегированных учетных записей ролей по системному администрированию, ролей по разработке и тестированию программных, программно-аппаратных средств, ролей администраторов безопасности.

5.24. Все действия по доступу пользователей с использованием привилегированных учетных записей подлежат регистрации. Контроль использования привилегированных учетных записей должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

5.25. Мероприятия по осуществлению мониторинга информационной безопасности должны предусматривать сбор данных о событиях безопасности, их обработке и анализе, а также выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации. Мероприятия по осуществлению мониторинга информационной безопасности должны проводиться в отношении всех ИС (АС, сетей), за исключением локальных и изолированных, в которых должен обеспечиваться контроль журналов регистрации событий безопасности. Мероприятия по мониторингу информационной безопасности должны осуществляться в соответствии с разделами 4 и 5 ГОСТ Р 59547-2021.

5.26. В ходе проведения мониторинга информационной безопасности для анализа зафиксированных событий безопасности и выявленных в них признаков реализации актуальных угроз допускается использование доверенных технологий искусственного интеллекта.

5.27. ЦБ (специалисты по защите информации подразделений) с периодичностью и в сроки, установленные внутренним регламентом по защите информации, должны представить ответственному лицу отчет о результатах мониторинга.

5.28. Мероприятия по разработке безопасного программного обеспечения должны быть направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом программном обеспечении в случае осуществления самостоятельной его разработки, при этом должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024 «Разработка безопасного

программного обеспечения. Общие требования».

5.29. Мероприятиями по обеспечению физической защиты ИС (АС) должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации. Физический доступ к программно-аппаратным средствам ИС (АС), предназначенным для обработки и хранения информации, должен быть предоставлен пользователям, которым указаный доступ необходим для выполнения возложенных на них обязанностей (функций). Программно-аппаратные средства ИС (АС), предназначенные для хранения информации, должны быть установлены в помещениях (зонах помещений, шкафах, футлярах, корпусах), несанкционированный физический доступ в которые должен быть исключен.

5.30. Контроль физического доступа к программно-аппаратным средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений, шкафы, футляры, корпуса), в которых они установлены, должен осуществляться в соответствии с внутренними регламентами по защите информации.

5.31. Съёмные МНИ, разрешенные для использования в ИС (АС, сетях), подлежат учету и контролю использования. В ИС (АС, сетях) должны использоваться съёмные МНИ, выдаваемые подразделением метрополитена. В случае обнаружения пользователем съёмного МНИ, принадлежность которого или владельца которого установить не удалось, такой съёмный МНИ должен быть передан в ЦБ для анализа содержащейся на нем информации, программ и при необходимости дальнейшего уничтожения. Подключение обнаруженного съёмного МНИ к ИС (АС, сетям) запрещается.

5.32. Посредством проведения мероприятий по обеспечению непрерывности функционирования ИС (АС, сетей) при возникновении нештатных ситуаций должна быть обеспечена возможность восстановления выполнения функций (процессов, видов работ), для которых метрополитеном установлены требования к непрерывному режиму функционирования, в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

5.33. Интервалы времени восстановления функционирования ИС (АС, сетей), их сегментов, выполняющих значимые функции, устанавливаются во внутренних стандартах и регламентах по защите информации в зависимости от значимости функций для обеспечения его деятельности, классов защищенности ИС (АС, сетей) и должны составлять:

– для ИС (АС) 1 класса защищенности – не более 24 часов с момента обнаружения нарушения функционирования;

- для ИС (АС) 2 класса защищенности – не более 7 календарных дней с момента обнаружения нарушения функционирования;
- для ИС (АС) 3 класса защищенности – не более 4 недель с момента обнаружения нарушения функционирования.

5.34. Программные, программно-аппаратные средства, позволяющие обеспечить выполнение значимых функций, должны быть развернуты в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный во внутренних стандартах и регламентах по защите информации интервал времени восстановления.

5.35. Подразделением – владельцем ИС (АС) должно быть обеспечено:

- создание достаточного количества резервных копий программных, программно-аппаратных средств и их конфигураций, обеспечивающих выполнение значимых функций, необходимых для восстановления выполнения значимых функций в установленный во внутренних стандартах и регламентах по защите информации интервал времени восстановления, и периодическое тестирование таких средств на работоспособность;

- создание достаточного количества резервных копий информации, необходимой для обеспечения выполнения значимых функций, а также их хранение на разных типах МНИ в местах, обеспечивающих исключение несанкционированный доступ к резервным копиям информации.

5.36. Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации определяются во внутренних стандартах и регламентах по защите информации.

5.37. Подразделение – владелец ИС (АС) должен организовывать периодические, но не реже одного раза в два года, проверки, в том числе в форме тренировок, возможности восстановления выполнения значимых функций с использованием резервных копий программных, программно-аппаратных средств и информации, необходимой для их выполнения, с привлечением работников, задействованных в проведении работ по восстановлению функционирования ИС (АС).

5.38. Мероприятия по повышению уровня знаний и информированности пользователей ИС (АС) по вопросам защиты информации должны включать:

- а) доведение до пользователей материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;
- б) проведение лекций, семинаров, обучающих игр по вопросам защиты информации;
- в) проведение имитационных рассылок электронных писем на служебные

адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;

г) проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

5.39. Применяемые способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний должны определяться во внутренних регламентах по защите информации. Оценка уровня знаний должна проводиться не реже одного раза в три года или после компьютерного инцидента. Для пользователей, у которых отсутствуют знания по вопросам защиты информации, должно быть организовано повторное прохождение обучающих курсов по вопросам защиты информации.

5.40. Мероприятий по защите информации при взаимодействии с подрядными организациями должны исключать возможность несанкционированного доступа или воздействий на ИС (АС) и содержащуюся в них информацию через взаимодействующие с ИС (АС) программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы, используемые для доступа подрядных организаций.

5.41. В отношении подрядной организации в договорных обязательствах должны быть установлены требования по обеспечению защиты информации, к которой получен доступ.

5.42. Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в документах, на основании которых подрядным организациям предоставлен доступ к ИС (АС).

5.43. В ИС (АС) подрядных организаций, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации. Состав информации, цели ее защиты и классы защищенности, в соответствии с которыми подрядными организациями должны быть приняты меры по защите информации во взаимодействующих ИС (АС), устанавливаются во внутренних стандартах и регламентах по защите информации.

5.44. Разработка и (или) тестирование ПО подрядными организациями непосредственно в эксплуатируемых ИС (АС) не допускается. Для проведения работ по разработке (развитию) и (или) тестированию ПО работникам подрядных организаций должен быть предоставлен доступ к выделенным для проведения таких работ стендам разработки и (или) тестирования, которые должны быть изолированы

от эксплуатируемых ИС (АС). Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования должен осуществляться в соответствии с внутренними регламентами по защите информации.

5.45. Мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании, должны исключить возможность блокирования авторизованным пользователям доступа к ИС (АС) и (или) содержащейся в них информации вследствие несанкционированных воздействий на интерфейсы, порты, сервисы, к которым должен быть обеспечен постоянный доступ из сети Интернет. Мероприятия, должны осуществляться с привлечением провайдеров хостинга или организаций, предоставляющих услуги связи, или организаций, оказывающих услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании. Программно-аппаратные средства, используемые для контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.

5.46. Должно быть обеспечено взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования.

5.47. Обеспечение доступности из сети Интернет интерфейсов и сервисов ИС (АС), подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, должно осуществляться в соответствии с внутренними регламентами по защите информации по согласованию с ЦБ после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с перечнем ресурсов сети Интернет, с которыми может взаимодействовать ИС (АС), включающим исходящий и входящий сетевые потоки, их характеристики и используемые протоколы.

5.48. При использовании для функционирования ИС (АС) искусственного интеллекта должна быть обеспечена возможность исключения несанкционированного доступа к информации или воздействия на ИС (АС), несанкционированного распространения и модификации информации, а также использования ИС (АС) не по их назначению за счет воздействия на наборы данных, применяемые модели искусственного интеллекта и их параметры, процессы и сервисы по обработке данных и поиску решений.

5.49. Не допускается передача лицу, разработавшему модель искусственного

интеллекта, информации ограниченного доступа, содержащейся в ИС (АС), в том числе для улучшения функционирования модели искусственного интеллекта.

5.50. При взаимодействии пользователей в целях выполнения ими своих обязанностей (функций) с сервисами на основе искусственного интеллекта посредством направления запроса и получения ответа должны быть:

а) при взаимодействии в формате строго заданных шаблонов запросов и ответов:

– определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам;

– определены шаблоны ответов искусственного интеллекта и обеспечен контроль соответствия ответов установленным шаблонам;

б) при взаимодействии в формате свободной текстовой формы запросов и ответов:

– определены для направляемых в искусственный интеллект запросов пользователей допустимые тематики и обеспечен контроль соответствия запросов допустимым тематикам;

– определены форматы ответов искусственного интеллекта в соответствии с допустимыми тематиками и обеспечен контроль соответствия ответов установленным форматам и допустимым тематикам;

в) разработаны статистические критерии для выявления недостоверных ответов искусственного интеллекта для последующего сбора и анализа недостоверных ответов;

г) обеспечено реагирование на недостоверные ответы искусственного интеллекта посредством ограничения области принимаемых решений и (или) реализации функций ИС (АС) на основе недостоверных ответов искусственного интеллекта.

5.51. При использовании в ИС (АС) искусственного интеллекта или сервисов на основе искусственного интеллекта должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование ИС (АС).

5.52. Непосредственно в состав ИС (АС) должны включаться доверенные технологии искусственного интеллекта или их компоненты.

5.53. Мероприятия по реализации в ИС (АС, сетях) мер по их защите и содержащейся в них информации должны включать:

1) реализацию базовых мер защиты ИС (АС, сетей) и содержащейся в них информации соответствующих классов защищенности;

2) адаптацию базовых мер защиты ИС (АС, сетей) и содержащейся в них информации применительно к архитектуре ИС (АС, сетей), применяемым информационным технологиям и особенностям функционирования;

3) верификацию адаптированного базовых мер защиты ИС (АС, сетей) и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

5.54. В ИС (АС, сетях) метрополитена должны быть реализованы следующие базовые меры их защиты и содержащейся в них информации:

- а) идентификация и аутентификация;
- б) управление доступом;
- в) регистрация событий безопасности;
- г) защита виртуализации и облачных вычислений;
- д) защита технологий контейнерных сред и их оркестрации;
- е) защита сервисов электронной почты;
- ж) защита веб-технологий;
- з) защита программных интерфейсов взаимодействия приложений;
- и) защита конечных устройств;
- к) защита мобильных устройств;
- л) защита технологий интернета вещей;
- м) защита точек беспроводного доступа;
- н) антивирусная защита;
- о) обнаружение и предотвращение вторжений на сетевом уровне;
- п) сегментация и межсетевое экранирование;
- р) защита от компьютерных атак, направленных на отказ в обслуживании;
- с) защита каналов передачи данных и сетевого взаимодействия.

5.55. Реализация мер по защите ИС (АС, сетей) и содержащейся в них информации, подлежащие реализации, должна обеспечивать защиту от нарушителей со следующими уровнями возможностей:

- в ИС (АС, сетях) 3 класса защищенности – от нарушителей с базовым уровнем возможностей;
- в ИС (АС, сетях) 2 класса защищенности – от нарушителей с повышенным уровнем возможностей;
- в ИС (АС, сетях) 1 класса защищенности – от нарушителей с высоким уровнем возможностей.

5.56. Мероприятия по контролю уровня защищенности информации, содержащейся в ИС (АС, сетях), должны обеспечивать включение проведения оценки возможностей нарушения безопасности информации и (или) нарушения

функционирования ИС (АС, сетей) внешними и внутренними нарушителями.

5.57. Контроль уровня защищенности информации должен проводиться в соответствии с внутренними регламентами по защите информации одним или совокупностью следующих методов:

а) автоматизированное и (или) ручное выявление уязвимостей ИС (АС, сетей) с последующей экспертной оценкой возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования систем;

б) выявление несанкционированных подключений устройств к ИС (АС, сетям);

в) тестирование ИС (АС, сетей) путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ним (воздействий на них) или повышения привилегий при реализованных мероприятиях и мерах по защите;

г) проведение в соответствии с планом тренировок по отработке работниками действий по обеспечению уровня защищенности информации, содержащейся в ИС (АС, сетях), в условиях реализации актуальных угроз.

5.58. Контроль уровня защищенности информации должен проводиться не реже одного раза в три года или после компьютерного инцидента. Методы контроля уровня защищенности информации и периодичность его проведения определяются во внутреннем регламенте.

5.59. По результатам проведения контроля уровня защищенности информации ЦБ разрабатывается отчет и представляется ответственному лицу для принятия при необходимости решения о выделении ресурсов с целью повышения уровня защищенности информации.

5.60. При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации в соответствии с настоящим Положением должны быть разработаны, обоснованы и внедрены компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных угроз (приложение № 2 к настоящему Положению).

## **6. Обязанности и права должностных лиц, осуществляющих мероприятия по информационной безопасности**

6.1. В соответствии с Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» ответственность за обеспечение информационной безопасности возложена на начальника метрополитена. Начальник метрополитена

утверждает «План мероприятий по совершенствованию защиты информации в ГУП «Петербургский метрополитен» и рассматривает отчетность о его исполнении.

6.2. Полномочия по обеспечению информационной безопасности в ГУП «Петербургский метрополитен», в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, реагированию на компьютерные инциденты, начальник метрополитена делегирует заместителю начальника метрополитена, ответственному за обеспечение информационной безопасности ГУП «Петербургский метрополитен» (далее – ответственное лицо за обеспечение информационной безопасности).

6.3. Полномочия права и обязанности ответственного лица за обеспечение информационной безопасности определены действующим «Положением о заместителе начальника метрополитена Санкт-Петербургского государственного унитарного предприятия «Петербургский метрополитен», ответственном за обеспечение информационной безопасности в ГУП «Петербургский метрополитен».

6.4. ЦБ выполняет функции по обеспечению информационной безопасности, определенные в соответствии с действующим «Положением о центре управления информационной безопасностью Управления метрополитена».

6.5. Ответственность за организацию работ по защите информации в проектируемых ИС (АС, сетях) возлагается на подразделение-заказчика или (и) участников жизненного цикла автоматизированного процесса (группы, команды проектов) в соответствии с их функциональными ролями, определенными в распорядительных документах метрополитена.

6.6. Подразделения, эксплуатирующие ИС (АС, сети), обязаны обеспечить выполнение мероприятий информационной безопасности, предусмотренных разделом 5 настоящего Положения в части их касающейся. Ответственность за обеспечение выполнения указанных мероприятий на объектах информатизации возлагается на руководителей подразделений, эксплуатирующих эти объекты.

6.7. За реализацию конкретных мер по защите информации в ИС (АС, сети) отвечают системные администраторы, администраторы безопасности и работники подразделений, в чьем ведении находятся объекты информатизации, имеющие соответствующие должностные обязанности и необходимую квалификацию в области защиты информации.

6.8. Работники, пользователи ИС (АС, сетей) метрополитена обязаны:

– знать и выполнять требования, изложенные в распорядительных документах, внутренних стандартах и регламентах по защите информации метрополитена и эксплуатационной документации на средства и СЗИ;

– незамедлительно сообщать об обнаружении признаков инцидентов информационной безопасности в соответствии с действующим Планом реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак.

6.9. По представлению ответственного лица, решением начальника метрополитена в подразделениях, эксплуатирующих ЗО КИИ, могут назначаться работники, на которых возлагаются отдельные функции по обеспечению безопасности ЗО КИИ. Обязанности, возлагаемые на работников, определяются в их должностных регламентах (инструкциях).

## **7. Взаимодействие по вопросам защиты информации**

7.1. Взаимодействие структурных подразделений метрополитена и ЦБ по вопросам защиты информации осуществляется на всех стадиях жизненного цикла ИС (АС, сети).

7.2. Порядок взаимодействия подразделений – заказчиков, рабочих групп, групп по изменениям ИС, команд проектов, других участников жизненного цикла в соответствии с их функциональными ролями определен в действующем «Формализованном регламенте жизненного цикла автоматизированного процесса предприятия».

7.3. Требования и документы по защите информации в ИС (АС, сети) подлежат согласованию с ответственным лицом.

7.4. ЦБ совместно с подразделениями-заказчиками, участвует в процессе выбора программно-аппаратных средств защиты информации, планируемых к приобретению и использованию в ИС (АС, сети), в подготовке программ и методик испытаний ИС (АС, сети) в части проверки реализации требований по защите информации, а также в проведении испытаний и опытной эксплуатации.

7.5. Взаимодействие со сторонними организациями – владельцами информационных систем, которые осуществляют информационный обмен с ИС (АС, сетями) метрополитена (внешними ИС), должно быть обеспечено на основании заключенного договора и (или) соглашения о конфиденциальности, а также действующих требований по подключению к информационной инфраструктуре метрополитена.

7.6. ЦБ по указанию ответственного лица взаимодействует по вопросам защиты информации с комитетами Правительства Санкт-Петербурга, территориальными и региональными подразделениями Регуляторов и организациями, предоставляющими услуги и выполняющими работы в области

защиты конфиденциальной информации в соответствии с требованиями законодательства Российской Федерации.

Подготовил:

Ведущий специалист сектора организации  
информационной безопасности и анализа  
центра управления информационной безопасностью  
Управления метрополитена

А.И. Васильев

СОГЛАСОВАНО

Начальник центра управления  
информационной безопасностью  
Управления метрополитена

И.С. Якутович

**Перечень централизованных мер защиты информации**

- 1) Идентификация и аутентификация субъектов и объектов доступа;
- 2) Управление доступом к информационным ресурсам;
- 3) Контроль привилегированных учетных записей;
- 4) Управление программной средой;
- 5) Управление мобильными устройствами пользователей;
- 6) Мониторинг информационной безопасности;
- 7) Управление компьютерными инцидентами в ИС (АС, сетях);
- 8) Антивирусная защита;
- 9) Контроль уровня защищенности ИС (АС, сетей);
- 10) Контроль конфигурации ИС (АС, сетей);
- 11) Резервное копирование и восстановление информации;
- 12) Мониторинг технического состояния, отказов программных и программно-технических средств;
- 13) Физическая защита объектов информатизации, контроль и управления доступом в помещения, в которых расположены программно-технические средства;
- 14) Защита от утечек информации в ИС (АС, сетях).

## **Примерный перечень компенсирующих мер защиты информации**

1. Компенсирующие меры, направленные на предотвращение возможности эксплуатации уязвимостей:

1.1. Изменение конфигурации уязвимых компонентов ИС, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

1.2. Ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей;

1.3. Резервирование компонентов ИС, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

1.4. Использование сигнатур, решающих правил СрЗИ, обеспечивающих выявление в ИС признаков эксплуатации уязвимостей;

1.5. Мониторинг информационной безопасности и выявление событий безопасности информации в ИС, связанных с возможностью эксплуатации уязвимостей.

2. Компенсирующие меры, направленные на нейтрализацию актуальных УБИ:

2.1. Замена части СрЗИ мерами физической защиты:

2.1.1. Ограничение физического доступа в помещения и к рабочим местам сотрудников, на которых осуществляется обработка информации;

2.1.2. Опечатывание/опломбирование системных блоков;

2.1.3. Опечатывание/опломбирование портов для подключения съемных устройств;

2.1.4. Использование имеющейся СКУД и системы видеонаблюдения.

2.2. Замена части средств защиты информации организационными мерами:

2.2.1. Ограничение, контроль и учет использования съемных носителей информации и мобильных устройств;

2.2.2. Запрет на использование пользователями административных учетных записей;

2.2.3. Утверждение перечней разрешенного и запрещенного ПО;

2.2.4. Ограничение использования сети Интернет путем определения перечня разрешенных для посещения сайтов;

2.2.5. Утверждение перечня пользователей, которым разрешен доступ к информации.

2.3. Использование встроенных механизмов защиты ОС:

2.3.1. Идентификация/аутентификация пользователей;

2.3.2. Разграничение доступа;

2.3.3. Ограничение программной среды;

2.3.4. Межсетевое экранирование;

2.3.5. Журналирование событий;

2.3.6. Шифрование дисков;

2.3.7. Отключение возможности загрузки с внешних носителей.

**Перечень нормативных правовых актов и методических документов по защите информации**

1. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
5. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».
7. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Доктрина информационной безопасности Российской Федерации».
9. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
10. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
11. Постановление Правительства Российской Федерации от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».
12. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием

атомной энергии и уполномоченном органе по космической деятельности».

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

14. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

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

16. Приказ ФСТЭК РФ от 11 апреля 2025 года № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

17. Приказ ФСТЭК РФ от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

18. Приказ ФСТЭК РФ от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

19. Приказ ФСТЭК РФ от 29 апреля 2021 года № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

20. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК РФ 15 февраля 2008 г.

21. «Методический документ. «Методика оценки угроз безопасности информации», утвержден ФСТЭК РФ 5 февраля 2021 г.

22. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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».

23. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

24. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности информации персональных данных, актуальные при обработке персональных данных информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждены руководством 8-го Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.

25. Государственные стандарты в сфере информации, информационных технологий и защиты информации:

25.1. «ГОСТ Р 51583-2014 Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утв. и введен в действие приказом Росстандарта от 28.01.2014 № 3-ст).

25.2. «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 373-ст).


25.3. «ГОСТ Р 59793-2021 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (утв. и введен в действие приказом Росстандарта от 25 октября 2021 г. N 1285-ст).


25.4. «ГОСТ 34.602-2020. Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (введен в действие приказом Росстандарта от 19.11.2021 № 1522-ст).

25.5. «ГОСТ Р 59711-2022. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами» (введен в действие приказом Росстандарта от 29 ноября 2022 года № 1377-ст).



## Лист согласования

Проект документа: «Положение о порядке организации и управления защитой информации в ГУП «Петербургский метрополитен»

Подготовил:  А.И. Васильев  
(ведущий специалист сектора организации информационной безопасности и анализа центра управления информационной безопасностью Управления метрополитена, тел. 2-82-71)

Проверил:  С.Ю. Цыпкина  
(техник 1 категории центра управления информационной безопасностью Управления метрополитена, тел. 2-53-32)

## СОГЛАСОВАНО

№	Подразделение	ФИО, должность	Результат (подпись)	Комментарий	Дата
1	Юридическая служба Управления метрополитена	 Аммиатов А.М.			04.12.25

Рассылка: НГУпр; НЗД; НЗКС; НЗРБ; НЗТ; НЗ-1; НЗК; НЗП; НЗЗ; НЗБ; НЗН; НЗЭ; ЦУС; СУРЭ; НМО; ЦТН; СБУФ; НПК; ЦЦР; КСУпр; ГДУпр; ЦТК; ЦБУпр; ЮСУпр; ЦАР; СУП; СРЗИ; ОБУпр; ПСУпр; ООУпр; ОНД; СЦУпр; ЦУИ; НСУпр; НПУпр; СИП; СГО; РБУпр; ОРС; Тупр; СОЗ; СВК; СТР; ДИП; СПАК; СМслужба; Делужба; Сслужба; ССР; ТЧ-2; СИТ; ТШслужба; ТЧ-7; ТЧ-1; ТЧ-5; Эслужба; ЭМслужба; СПБ; СТС; ТЧ-3; Пслужба; ЭСслужба; ОМЧ; НХслужба; ТЧ-6; САР; СМО; СТБ; ПКТБ; ССД; Шслужба; АТП; ТЧ-4; СПС