ФГБОУ ВО СИБИРСКАЯ
ПОЖАРНО-СПАСАТЕЛЬНАЯ
АКАДЕМИЯ ГПС МЧС РОССИИ

С.В. Бабенышев
Е.Н. Матеров

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЧС

Учебное пособие

Железногорск

МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

ФГБОУ ВО СИБИРСКАЯ ПОЖАРНО-СПАСАТЕЛЬНАЯ АКАДЕМИЯ ГПС МЧС РОССИИ

Бабенышев С.В., Матеров Е.Н.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЧС

Учебное пособие

«Допущено ФГБОУ ВО Сибирская пожарно-спасательная академия Государственной противопожарной службы МЧС России в качестве учебного пособия»

Железногорск
2024

УДК 004.9 + 004.7
ББК 16.33
Б12

Авторы:
Бабенышев Сергей Валерьевич, канд. физ.-мат. наук
Матеров Евгений Николаевич, канд. физ.-мат. наук

Рецензенты:
Волокобинский Михаил Юрьевич, ппрофессор, доктор технических наук
(ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России)

Тетерин Иван Михайлович, профессор, доктор технических наук
(ФГБОУ ВО Академия ГПС МЧС России)

Бабенышев, С.В. Информационные технологии поддержки принятия решений в чрезвычайных ситуациях [Текст]: учебное пособие / С.В. Бабенышев, Е.Н. Матеров. – Железногорск: ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2024. – 145 с.: ил.

Учебное пособие содержит методически систематизированный материал, охватывающий темы учебной программы дисциплины «Информационные технологии поддержки принятия решений в чрезвычайных ситуациях». В нем особое внимание уделено действующей нормативной базе, на основе которой происходит принятие решений в области чрезвычайных ситуаций (ЧС), тенденциям законодательных изменений, применению свободно распространяемых программных средств, имеющимся информационным системам поддержки принятия решений. Пособие предназначено для использования в образовательном процессе Сибирской пожарно-спасательной академии ГПС МЧС России при изучении учебной дисциплины «Информационные технологии поддержки принятия решений в ЧС» обучающимися по направлению подготовки 38.03.04 Государственное и муниципальное управление.

УДК 004.9 + 004.7
ББК 16.33

ISBN 978-5-906874-82-5

Оглавление

ПРЕДИСЛОВИЕ

Активное внедрение информационных технологий в деятельность МЧС России требует постоянного обновления учебных программ для подготовки кадров органов управления, способных эффективно взаимодействовать с ЦУКСами при устранении последствий чрезвычайных ситуаций (ЧС). Из года в год информационные инструменты, используемые в ЦУКСах, обновляются, внедряются новые информационные системы, алгоритмы и методики. В сфере информационной поддержи принятия решений в чрезвычайных ситуациях необходимый функционал интенсивно наращивается добавлением новых программных решений, в том числе и от коммерческих поставщиков. Столь быстрые изменения из-за инерционности, внутренне присущей учебному процессу, создают вызовы для учебных заведений в деле поддержки актуальности учебных материалов соответствующих учебных дисциплин. Традиционным решением является разделение учебного материала на относительно неизменные основы и, подверженные частым изменениям, примеры применений.

Еще одной важной причиной значительных сдвигов в сфере информационных технологий, в том числе применяемых при управлении в чрезвычайных ситуациях, является санкционный фактор и тенденция на увеличение международной напряженности. В силу сложившихся исторических обстоятельств, информационные технологии, включая самые передовые программные технологии, такие как облачные, технологии искусственного интеллекта, интернета вещей и т.д. получали развитие сначала за рубежом, причем как коммерческие, так и свободно распространяемые, последние часто воспринимаются как средства ухода от санкционного контроля. Это позволяет, опираясь на санкционный режим, контролировать и произвольно ограничивать распространение современных программных средств в Российской Федерации из-за рубежа. Обладая технологическими ключами к программным продуктам, недобросовестные поставщики программного обеспечения могут использовать их для разведки, взлома, и перехвата управления технологическими объектами (Глава 6).

Третьей, и, по сути, основной, причиной динамичных изменений технологического «ландшафта» сферы информационных технологий является активное развитие информационных технологий самих по себе, обещающее большие сдвиги во всех сферах человеческой жизни, и, в частности, в сферах

мониторинга природных процессов, управления техносферными объектами, в сфере государственного управления.

Перечислим несколько перспективных программных технологий, включая как уже реализованные алгоритмы обработки данных, так и информационные системы, позволяющие использовать получаемые данные в интересующих нас целях:

- Построение 3D-модели разрушений жилого или производственного здания, по данным собираемым во время облета БАС, что позволяет оперативно руководить спасательными действиями.
- Мониторинг смещений грунта или снега на горных склонах и коммунальных отвалах по смещению маячков с помощью БАС для предсказания оползней.
- Задачи оптимальной логистики в условиях нарушения целостности и ограничений проходимости дорожной сети.
- Построение ортофотопланов для определения границ затоплений в целях определения зоны ЧС и оперативной выплаты компенсаций пострадавшим.

Учебное пособие состоит из 7 глав, соответствующих темам рабочей программы дисциплины, введения и заключения:

Глава 1 «Основные используемые в МЧС России информационные системы» содержит перечень и описание базовых информационных систем, используемых в органах повседневного управления МЧС России при профилактике, мониторинге и ликвидации ЧС. Также обсуждаются зарубежные информационные системы и проблемы, связанные с их использованием.

Глава 2 «Автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» содержит информацию по АИУС РСЧС и законодательных тенденциях ее функционирования.

Глава 3 «Системы мониторинга» рассматривает принципы организации программных систем используемых для мониторинга ЧС.

Глава 4 «Системы поддержки принятия решений» дает обзор применений информационных технологий для поддержки принятия решений в профилактике, предупреждении, мониторинга развития и ликвидации ЧС.

Глава 5 «Географические информационные системы» представляет собой краткий обзор существующих ГИС и их возможностей, останавливаясь подробно

на примерах их применения в ликвидации ЧС. Здесь же обсуждаются возможные открыто распространяемые и российские альтернативы.

Глава 6 «Компьютерные сети» излагает основные принципы организации компьютерных сетей и связанных с ними проблем безопасности.

Глава 7 «Защита информации в информационных технологиях» акцентирует внимание на операционных системах семейства Линукс и специальной ОС Astra Linux, формулирует основные принципы организации контроля доступа и обеспечения безопасности в этих системах.

Пособие состоит из 145 страниц и содержит 51 библиографическую ссылку.

Первоначальная верстка пособия выполнена с помощью свободно распространяемой издательской системы Quarto.

ВВЕДЕНИЕ

Развитие информационных технологий в областях интернета вещей (англ. *internet of things*, IoT), обработки больших данных, алгоритмов машинного и глубокого обучения дает возможность существенного прогресса в деле профилактики, предотвращения, раннего выявления, мониторинга и ликвидации чрезвычайных ситуаций (ЧС). В частности, возникающие технологии интернета вещей позволяют развертывать масштабные экономичные сети сенсоров и датчиков, там, где ранее приходилось полагаться на квалифицированный персонал, где риски связанны с человеческим фактором. Для обработки массива поступающих данных необходимы технологии обработки больших данных, машинного и глубокого обучения. Указанные области развития предоставляют беспрецедентные возможности развития автоматизированных систем поддержки принятия решения на всех этапах возникновения и развития широкого спектра чрезвычайных ситуация. Пока не приходится говорить о полностью автоматических системах ввиду законодательных ограничений и известной недостаточной зрелости соответствующих технологий. Далее приводится краткий обзор номенклатуры источников ЧС и перспектив использования информационных технологий.

Согласно действующему ГОСТ 22.0.06-97/ГОСТ Р 22.0.06-95 «Безопасность в чрезвычайных ситуациях. Источники природных чрезвычайных ситуаций. Поражающие факторы. Номенклатура параметров поражающих воздействий»[1], к опасным природным явлениям и процессам относятся:

- опасные геофизические явления (извержения вулканов, землетрясения);

  Замечание. Землетрясения являются наиболее опасными видом ЧС в виду масштабности, быстрого развития, невозможности предупреждения и отсутствия надежных технологий предсказания.

- опасные геологические явления (оползни, обвалы, осыпи; карстовая просадка (провал) земной поверхности, просадка лессовых пород; абразия; эрозия, склоновый смыв; курумы);

  Замечание. Предсказание оползней и осыпей возможно, но требует мониторинга состояния и движений грунта. Наименее затратные современные технологии используют маркерные флажки и БАС для выявления смещений грунта. Надежное предсказание и предупреждение может осложняться погодными явлениями – сильными дождями или морозами, небольшими сейсмическими толчками, в том числе и

[1] Вместо ГОСТ 22.0.06-97 с 01.02.2024 вводится Межгосударственный ГОСТ 22.0.06-2023 [1].

техногенного происхождения. По характеру проявлений сюда же можно отнести оползни на полигонах коммунальных отходов, приводящих к выделению токсичных газов, угрожающих здоровью населения.

- опасные метеорологические явления (сильный ветер, в т.ч. шквал, смерч; очень сильный дождь (мокрый снег, дождь со снегом); сильный ливень (очень сильный ливневый дождь); продолжительные сильные дожди; очень сильный снег; крупный град; сильная метель; сильная пыльная (песчаная) буря; сильное гололедно-изморозевое отложение на проводах; сильный туман; сильный мороз; сильная жара; заморозки; засуха; сход снежных лавин);

  Замечание. Традиционно, метеорологические явления трудно поддаются среднесрочному и долговременному прогнозу, а предсказания отдельных явлений, таких как сильный и шквальный ветер, ливневые дожди, град, имеют проблемы с точной локализацией, отчего снижается эффективность системы предупреждения, из-за эффекта психологической усталости населения. Возможна эффективная профилактика снежных лавин, но требуется профессиональный мониторинг сопутствующих факторов: уровня снежного покрова, погоды.

- морские опасные гидрометеорологические явления (цунами, тропические циклоны (тайфуны), сильное волнение (5 баллов и более), сильный тягун в морских портах; обледенение судов; сгонно-нагонные явления; раннее появление льда, интенсивный дрейф льда, сжатие льда, сильный туман на море, непроходимый, труднопроходимый лед, навалы льда на берега и морские гидротехнические сооружения; отрыв прибрежных льдин с людьми);

  Замечание. Морские цунами являются еще одним примером трудно предсказуемых быстроразвивающихся ЧС чрезвычайно разрушительного потенциала. Несмотря на то, что появлению цунами обычно предшествуют заранее регистрируемые сейсмические толчки, до сих пор нет надежного способа предсказать, когда землетрясение вызовет цунами, а когда нет. Это снижает эффективность мер оповещения населения. Опасность цунами не ограничивается приморскими территориям. Редкое природное явления – ледяное цунами произошло в долине реки Бурея году в 2018 в результате крупного оползня. Вызванная оползнем волна воды, смешанной со льдом, достигла высоты почти 50 м и прошла на 12 км вверх и немного меньше вниз по течению реки. Только малонаселенность территории спасла от масштабных человеческих жертв и экономических потерь. Основной причиной указывается обводнение грунтов в нижней части оползневого склона при заполнении водохранилища Бурейской ГЭС [2].

- опасные гидрологические явления (высокие уровни воды (половодье, зажор, затор, дождевой паводок), сель, низкие уровни воды (низкая межень), раннее льдообразование);

  Замечание. Гидрологические причины ЧС являются гораздо меньшей проблемой на реках с регулируемым стоком (то есть, где имеются плотины или дамбы), но не полностью исключаемой, как было в сезон высокой воды на реке Енисей в 2021 году. Тем не менее, процессы спуска воды с дамб или плотин являются более предсказуемыми и медленно развивающимися. Из великих рек России остается нерегулируемой только Лена, опасностям половодий и сопутствующих явлений вроде заторов (крупного льда) или зажоров (шуги и мелкого льда) на Лене уделяется большое внимание в работе НЦУКС. Как правило для понимания процессов половодий требуются масштабные гидрологические исследования на каждом опасном участке реки, учитывающие рельеф дна, водный режим, динамические процессы и т.п. С другой стороны, на реках с регулируемым стоком появляется опасность техногенных гидродинамических ЧС, связанных с нарушением целостности или разрушением плотин и дамб, как было продемонстрировано техногенной катастрофой (погибло 75 человек) на Саяно-Шушенской в 2009 год, когда в результате разрушения агрегатов произошло обесточивание станции, и только героическими усилиями персонала станции были предотвращены более масштабные гидродинамические последствия для территорий вниз по течению. Другим примером гидродинамического ЧС является недавняя катастрофа в Херсонской области. Для предотвращения таких ЧС на объектах инфраструктуры используются системы информационного мониторинга, собирающие и анализирующие показания промышленных датчиков температуры оборудования, вибрации, электротехнических характеристик оборудования и т.д.

- природные пожары (лесные пожары, торфяные пожары, пожары на оленьих пастбищах).

  Замечание. Природные пожары представляют серьезную опасность не только для малонаселенных лесных пространств Сибири и Дальнего востока, но и, как показывают события весны 2023 года в Свердловской (2 погибших) и Курганской области (19 погибших), для Европейской части России и Урала. Подобные пожары становятся особенно смертоносными, если сопровождаются штормовой погодой и шквалистым ветром. В настоящее время, для расчета комплексного показателя пожароопасности территории используется индекс Нестерова, разработанный в 1949 году. Несмотря на известные недостатки и неточность, индекс Нестерова обязателен к применению, что закреплено в ГОСТ Р 22.1.09-99.2000. Попытки разработки более современных подходов, использующих площадные погодные данные, в том числе, полученные и по результатам компьютерного моделирования, наталкиваются на общую неопределенность гидрометеорологических прогнозов.

Причинами биолого-социальных ЧС становятся:

- инфекционные, паразитарные болезни и отравления людей (особо опасные болезни (холера, чума, туляремия, сибирская язва, мелиоидоз, лихорадка Ласса, болезни, вызванные вирусами Марбурга и Эбола), опасные кишечные инфекции (болезни I и II группы патогенности), инфекционные заболевания людей невыясненной этиологии, отравления людей, эпидемии);
- особо опасные болезни сельскохозяйственных животных и рыб (особо опасные острые инфекционные болезни сельскохозяйственных животных: ящур, бешенство, сибирская язва, лептоспироз, туляремия, мелиоидоз, листериоз, чума (КРС, МРС), чума свиней, болезнь Ньюкасла, оспа, контагиозная плевропневмония, прочие острые инфекционные болезни сельскохозяйственных животных, хронические инфекционные болезни сельскохозяйственных животных (бруцеллез, туберкулез, лейкоз, сап и др.), экзотические болезни животных и болезни невыясненной этиологии, массовая гибель рыб);
- карантинные и особо опасные болезни и вредители сельскохозяйственных растений и леса.

К техногенным ЧС относят взрывы, пожары, аварии на радиоактивно и химически опасных объектах, выбросы радиоактивных и химически опасных веществ, патогенных для человека микроорганизмов, обрушение зданий, аварии на системах жизнеобеспечения, транспортные аварии и др. Отдельно выделяются аварии на электроэнергетических системах, коммунальных системах жизнеобеспечения, очистных сооружениях и гидродинамические аварии.

Классификация ЧС в зависимости от масштаба и тяжести последствий

По масштабам распространения и тяжести последствий ЧС делятся на чрезвычайные ситуации локального, муниципального, межмуниципального, регионального, межрегионального и федерального характера (Таблица 1) [3].

Таблица 1 – Характер чрезвычайных ситуация

Характер ЧС	Масштаб распространения и тяжесть последствий
а) локальный	территория, на которой сложилась чрезвычайная ситуация и нарушены условия жизнедеятельности людей (далее – зона чрезвычайной ситуации), не выходит за пределы территории объекта, при этом количество людей, погибших или получивших ущерб здоровью (далее – количество

Характер ЧС	Масштаб распространения и тяжесть последствий
	пострадавших), составляет не более 10 человек либо размер ущерба окружающей природной среде и материальных потерь (далее – размер материального ущерба) составляет не более 100 тыс. рублей
б) муниципальный	зона чрезвычайной ситуации не выходит за пределы территории одного поселения или внутригородской территории города федерального значения, при этом количество пострадавших составляет не более 50 человек либо размер материального ущерба составляет не более 5 млн. рублей, а также данная чрезвычайная ситуация не может быть отнесена к чрезвычайной ситуации локального характера
в) межмуниципальный	зона чрезвычайной ситуации затрагивает территорию двух и более поселений, внутригородских территорий города федерального значения или межселенную территорию, при этом количество пострадавших составляет не более 50 человек либо размер материального ущерба составляет не более 5 млн. рублей
г) региональный	зона чрезвычайной ситуации не выходит за пределы территории одного субъекта Российской Федерации, при этом количество пострадавших составляет свыше 50 человек, но не более 500 человек либо размер материального ущерба составляет свыше 5 млн. рублей, но не более 500 млн. рублей
д) межрегиональный	зона чрезвычайной ситуации затрагивает территорию двух и более субъектов Российской Федерации, при этом количество пострадавших составляет свыше 50 человек, но не более 500 человек либо размер материального ущерба составляет свыше 5 млн. рублей, но не более 500 млн. рублей
е) федеральный	количество пострадавших составляет свыше 500 человек либо размер материального ущерба составляет свыше 500 млн. рублей

Природные и техногенные ЧС

Способы прогнозирования, профилактики, предотвращения, мониторинг развития и устранение последствий ЧС существенно зависят от вида самой ЧС. К природным явлениям на территории России, которые могут привести к массовым человеческим жертвам, значительному ущербу здоровью населения и материальному ущербу относятся быстроразвивающиеся события, такие как,

землетрясения, цунами, наводнения, оползни, природные (ландшафтные) пожары. Медленно протекающие природные явления, например, засухи или опускание прибрежных зон представляют меньшую угрозу.

Далее рассмотрим более подробно опасные природные явления, которые в силу своей природы и масштабности, как правило невозможно предотвратить и которые до сих пор плохо поддаются прогнозированию.

Землетрясения

Российские территории, подверженные опасностям землетрясений (сейсмически опасные зоны) расположены на Северном Кавказе, Алтае, в Прибайкалье.

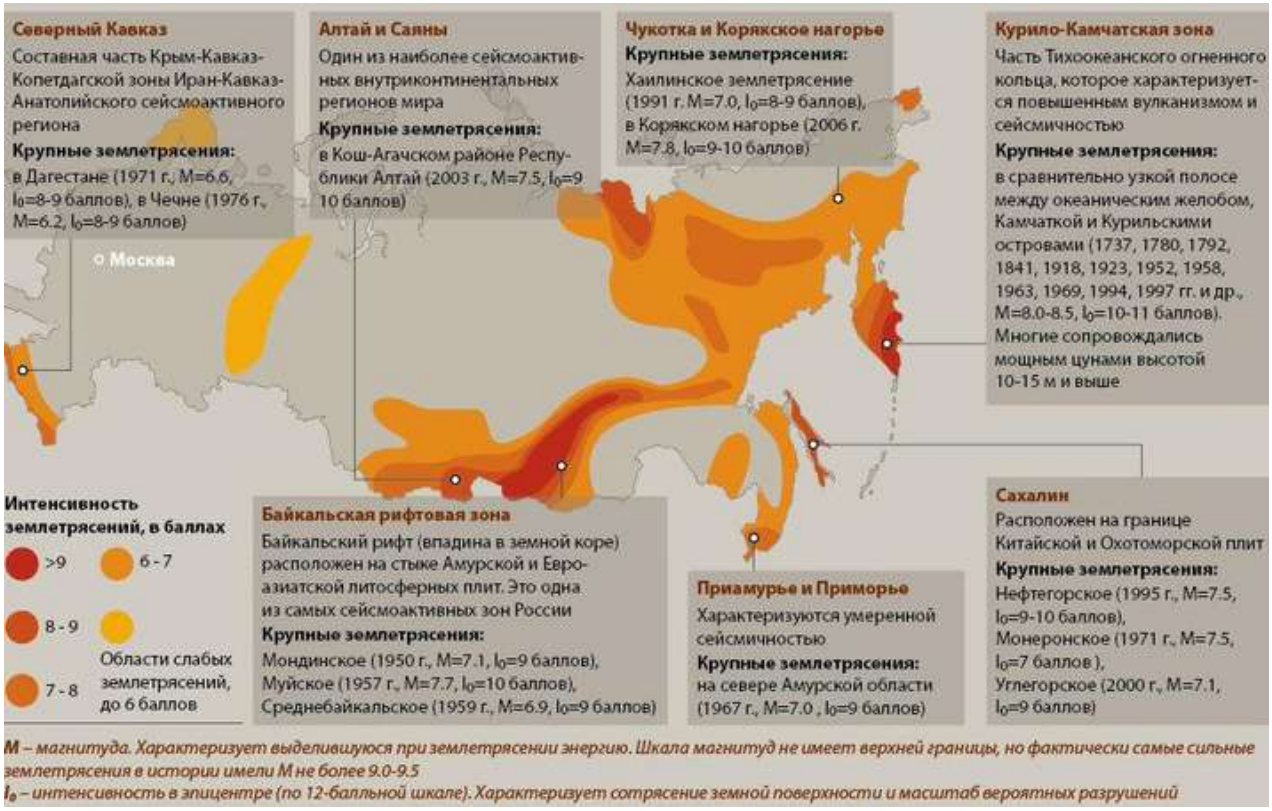

Рисунок В.1. – Локализации сейсмически активных зон России.
(Источник: сайт Института физики Земли им. О.Ю. Шмидта РАН)

Предсказать точно время землетрясений пока не представляется возможным – до сих пор не существует методов даже краткосрочного прогноза. Тем не менее, разрабатываются подходы хотя бы для локализации вероятной области очага с точностью до нескольких километров, например, метод, использующий совокупный анализ вариаций микросейсмических шумов в низком диапазоне частот и деформаций горных пород и требующий наличия

нескольких сейсмостанций, находящихся в разных азимутах от эпицентра землетрясения.

Крупнейшее землетрясение произошло на Сахалине в 1995 году, когда в течении 17 секунд оказался полностью разрушен поселок Нефтегорск – 17 блочных пятиэтажных домов на 80 квартир, несколько двухэтажных жилых зданий, детский сад, школа, клуб. Из 3 197 человек населения поселка погибло 2 040. Причем до катастрофы Сахалин считался сейсмически умеренно опасным.

В районе озера Байкал, которое расположено по глубинному разлому протяженностью около 1 500 километров, во время Цаганского землетрясения, в 1862 году магнитуда достигла 7,5 балла. Тогда в дельте реки Селенга под воду ушло около 200 квадратных километров суши.

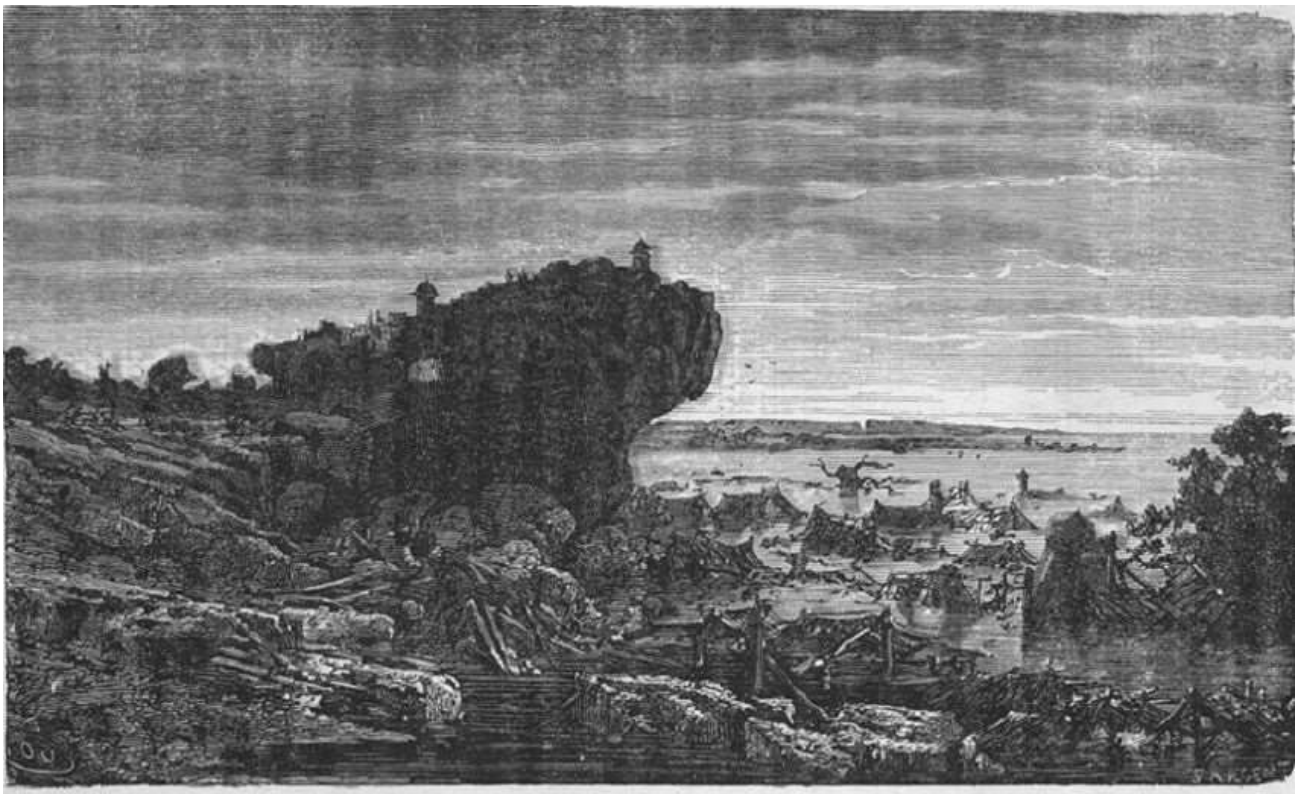

Рисунок В.2. – Последствия Цаганского землетрясения 1862 года на Байкале. (Гравюра из книги "Путешествие по Амуру и Восточной Сибири", 1868 г)

Цунами

В Российской Федерации угрозе цунами наиболее подвержены населенные пункты приморских территорий Сахалинской области, Камчатского края и Приморского края. На этих территория проживает большая часть населения и

сосредоточен основной экономический потенциал Российского Дальнего Востока.

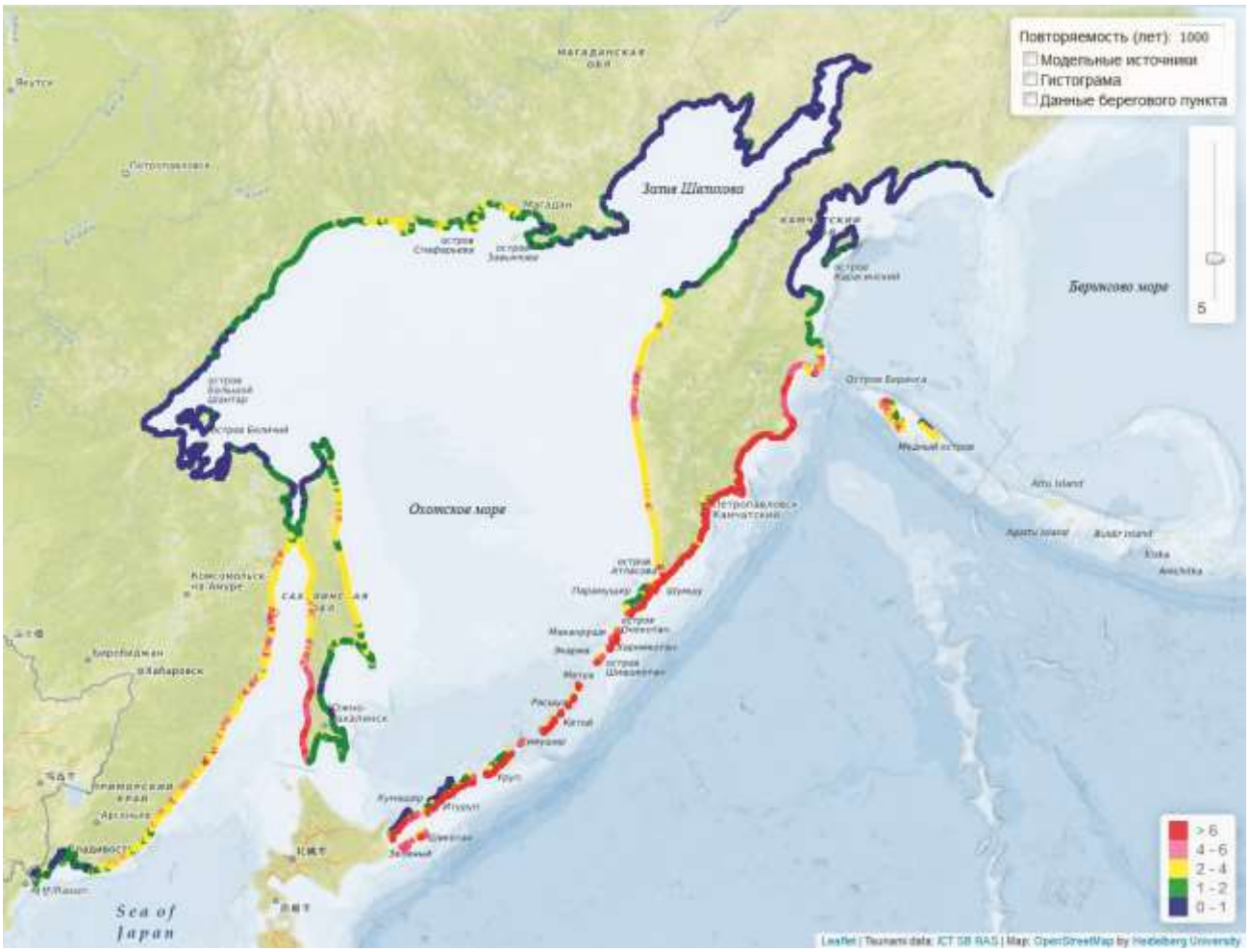

Рисунок В.3. – Карта цунами-опасности на Дальнем востоке России. (Источник: ИВТ СО РАН, ИВМиМГ СО РАН)

Волны сюда приходят из, так называемой, цунамигенной зоны, расположенной в Курило-Камчатском и Алеутском желобах, а также может приходить от удаленных землетрясений, так, например, в 1960 году волна высотой 6-7 метров подошла к побережью Камчатки в результате цунами, возникшего почти сутками ранее у берегов Чили [4]. Цунами силой 4 балла повторяются в среднем раз в 50-100 лет, более слабые – в 10 раз чаще. Наиболее разрушительное в российской истории цунами произошло в октябре 1952 года, когда почти полностью был разрушен город Северо-Курильск, погибли около 14 тысяч человек [5]. Отметим, что следы от цунами (порядка 50 случаев за последние 2 500 лет) отмечаются и в Причерноморье [6].

Для своевременного выявления и предупреждения населения создана интегрированная международная информационная система оповещения о

цунами, включающая автоматизированные посты инструментальных наблюдений за уровнем моря.

Чрезвычайные ситуации техногенного характера

К техногенным событиям относятся: крупные пожары, взрывы бытового газа, пожары и взрывы на нефте- и газопроводах и многие другие. В связи с последними событиями, к ним добавились давно отсутствовавшие риски ЧС, связанные с последствиями от военных действий. Сложность ликвидации последствий таких ЧС связана с дополнительными факторами, такими как, угроза от неразорвавшихся боеприпасов и вероятность повторного огневого налета.

Стадии (фазы) развития чрезвычайной ситуации

Чрезвычайная ситуация любого типа в своем развитии проходит четыре типовые стадии (фазы) (Таблица 2):

Таблица 2 – Стадии развития ЧС

Стадии (фазы) развития ЧС	**Описание**
предварительная	образуются и нарастают предпосылки к возникновению природного или техногенного бедствия, накапливаются отклонения от нормального состояния или процесса
первая	инициирование природного или техногенного бедствия и последующее развитие процесса чрезвычайного события, во время которого оказывается воздействие на людей, объекты экономики, инфраструктуры и природную среду
вторая	осуществляется ликвидация последствий природного или техногенного бедствия, ликвидация чрезвычайной ситуации (эта стадия может начинаться и до завершения первой стадии)
третья	осуществляется ликвидация долговременных последствий природного и техногенного бедствия

Режимы функционирования органов управления РСЧС

От точной классификации, возникшей или вероятной ЧС, зависит режим функционирования и порядок деятельности органов управления и сил РСЧС [7]. Напомним, что РСЧС состоит из территориальных и функциональных подсистем. Территориальные подсистемы создаются в субъектах РФ для предупреждения и ликвидации чрезвычайных ситуаций в пределах их

территорий и состоят из звеньев, соответствующих административно-территориальному делению этих территорий. Функциональные подсистемы создаются федеральными органами исполнительной власти для организации работы по защите населения и территорий от чрезвычайных ситуаций в сфере их деятельности и порученных им отраслях экономики.

Режим функционирования органов управления и сил РСЧС – это определяемые в зависимости от обстановки, прогнозирования угрозы ЧС и возникновения ЧС, порядок организации деятельности органов управления и сил Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее – РСЧС) и основные мероприятия, проводимые указанными органами управления и силами в режиме повседневной деятельности, при установлении режима повышенной готовности или чрезвычайной ситуации.

В соответствии со статьей 4.1 Федерального закона от 21.12.94 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [7], при отсутствии угрозы возникновения ЧС на объектах, территориях или акваториях органы управления и силы РСЧС функционируют в режиме повседневной деятельности.

Комиссия по чрезвычайным ситуациям субъекта (КЧС) является координирующим органом территориальной подсистемы РСЧС и предназначена для организации и выполнения работ по предупреждению чрезвычайных ситуаций, уменьшению ущерба при их возникновении и ликвидации их последствий, а также координации деятельности по этим вопросам предприятий, организаций и учреждений, расположенных на территории субъекта, независимо от ведомственной принадлежности и форм собственности.

Решениями руководителей федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, органов местного самоуправления и организаций, на территории которых могут возникнуть или возникли ЧС, либо к полномочиям, которых отнесена ликвидация ЧС, для соответствующих органов управления и сил РСЧС может устанавливаться один из следующих режимов функционирования (Таблица 3):

Таблица 3 – Режимы функционирования органов РСЧС

Режим функционирования	**Условия**
повседневной деятельности	отсутствие угрозы возникновения ЧС
повышенной готовности	при угрозе возникновения ЧС
чрезвычайной ситуации	при возникновении и ликвидации ЧС

Критерии отнесения к чрезвычайным ситуациям

Приказ МЧС России от 5 июля 2021 г. № 429 «Об установлении критериев информации о чрезвычайных ситуациях природного и техногенного характера» (вступил в силу с 1 января 2022 года) определяет следующие критерии отнесения события к ЧС (Таблица 4):

Таблица 4 – Признаки чрезвычайных ситуаций

№ п/п	Наименование источника ЧС	Критерии отнесения события к ЧС
1.	**Техногенные чрезвычайные ситуации**	
1.1.	Транспортные аварии	
1.1.1.	Аварии на метрополитене	1. Столкновение подвижного состава с другим подвижным составом, сход подвижного состава на главных путях перегонов и станций, в результате которого: погиб 1 человек и более; или получили вред здоровью, за исключением поверхностных повреждений (в том числе ссадины, кровоподтека, ушиба мягких тканей, включающего кровоподтек и гематому), поверхностных ран и других повреждений, не влекущих за собой кратковременное расстройство здоровья или незначительную стойкую утрату общей трудоспособности (далее - вред здоровью), 5 человек и более. 2. Полный перерыв в движении поездов на 5 часов и более в результате аварии.
1.1.2.	Аварии на железнодорожном транспорте	1. Столкновение железнодорожного подвижного состава с другим железнодорожным подвижным составом, с транспортным средством, сход железнодорожного подвижного состава на перегоне или железнодорожной станции, при поездной или маневровой работе, экипировке или других передвижениях (за исключением случаев гибели или причинения тяжкого вреда здоровью людям, не являющимся работниками железнодорожного транспорта и (или) пассажирами, вследствие столкновения железнодорожного подвижного состава с транспортным средством), в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или установлен факт нарушения условий жизнедеятельности в результате воздействия поражающих факторов источника чрезвычайной ситуации (далее – нарушены условия жизнедеятельности) 50 человек и более; или произошел разлив топлива и иных загрязняющих веществ на почву в объеме 5 т и более.

		2. Полный перерыв движения поездов на перегоне и (или) железнодорожной станции с прекращением пассажирского сообщения на 6 часов и более.
1.1.3.	Аварии на монорельсовом транспорте	1. Столкновение подвижного состава с другим подвижным составом, сход подвижного состава на главных путях перегонов и станций, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более. 2. Полный перерыв в движении на 5 часов и более в результате аварии.
1.1.4.	Аварии на подвесной и наземной канатной дороге транспортной	Событие, повлекшее разрушение или повреждение конструкции подвесной канатной дороги транспортной и (или) наземной канатной дороги транспортной (в том числе от воздействия внешних факторов), в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или перерыв в работе на 6 часов и более (при отсутствии альтернативных путей быстрой доставки людей иным наземным транспортом).
1.1.5.	Аварии на автомобильном транспорте	1. Дорожно-транспортное происшествие с участием автотранспортного средства, осуществляющего пассажирские перевозки и имеющего более восьми сидячих мест, помимо сидения водителя, в результате которого: погибли 5 человек и более; или получили вред здоровью 10 человек и более. 2. Прекращение или ограничение движения на участке дороги (федерального и регионального значения), не имеющей объездных путей, на 6 часов и более.
1.1.6.	Аварии на водном транспорте	Столкновение, опрокидывание, затопление, посадка на мель, выбрасывание на берег судов (в том числе вследствие неблагоприятных гидрометеорологических условий), в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или затруднено (прекращено) судоходство на 72 часа и более; произошел разлив топлива и попадание загрязняющих веществ в водный объект в объеме 1 т и более.
1.1.7.	Аварии на воздушном транспорте	Авиационное событие (катастрофа, авария), за исключением событий со сверхлегкими судами (максимальная взлетная масса которых составляет не более 495 кг без учета массы авиационных средств спасания), в результате которого:

		погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более.
1.1.8.	Ракетно-космические катастрофы и аварии на стартовых комплексах и в населенных пунктах и вне стартовых комплексов и населенных пунктов	Падение, разрушение ракетно-космического изделия (космического аппарата) - любой факт.
1.2.	Взрывы (в том числе с последующим горением) и (или) разрушения (обрушения) в зданиях и сооружениях	
1.2.1.	Взрывы и (или) разрушения (обрушения) в зданиях, сооружениях, предназначенных для постоянного или длительного (круглосуточного) проживания людей	Взрыв и (или) полное или частичное внезапное разрушение (обрушение) зданий и сооружений, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности5 1 человека и более.
1.2.1.	Взрывы и (или) разрушения (обрушения) в зданиях, сооружениях, предназначенных для постоянного или длительного (круглосуточного) проживания людей	Взрыв и (или) полное или частичное внезапное разрушение (обрушение) зданий и сооружений, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности[5] 1 человека и более.
1.2.2.	Взрывы и (или) разрушения (обрушения) в зданиях, сооружениях, предназначенных для временного пребывания людей, преимущественно ритмичного характера (рабочий день, школьная смена, сеанс и т.д.)	Взрыв и (или) разрушение (обрушение) элементов зданий и сооружений, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более.

1.2.3.	Взрывы и (или) разрушения (обрушения) в зданиях, сооружениях, предназначенных для производственного или складского назначения	Разрушение сооружений и (или) технических устройств, применяемых на опасном производственном объекте[6], неконтролируемый взрыв и (или) выброс опасных веществ, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более.
1.2.4.	Взрывы и (или) разрушения (обрушения) открытых и крытых спортивно-физкультурных, зрелищных, торговых сооружений (стадионы, спортивно-развлекательные комплексы, рынки)	Взрыв и (или) внезапное разрушение (обрушение) зданий и сооружений, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более.
1.2.5.	Разрушения (обрушения) элементов транспортной и инженерной инфраструктуры (мосты и тоннели длиной 500 м и более)	Внезапное разрушение (обрушение) элементов транспортной, инженерной инфраструктуры, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более; или произошло прекращение (ограничение) движения на участке дороги, не имеющей объездных путей, на 6 часов и более; или произошло обрушение транспортных и инженерных конструкций в водный объект.
1.2.6.	Аварии на объектах ведения горных работ (шахты, подземные и горные выработки)	Внезапное обрушение горных пород, затопление, внезапный выброс газа и угля (породы), превышение концентрации газа, взрыв, разрушение технических устройств, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более.
1.3.	Аварии на системах жизнеобеспечения	
1.3.1.	Аварии на объектах теплоснабжения	Нарушены условия жизнедеятельности 50 человек и более на 1 сутки и более при условии: температура

		воздуха в жилых комнатах более суток фиксируется ниже +18°С в холодный период (теплый период - ниже +20°С)[7].
1.3.2.	Аварии на объектах водоснабжения, электроэнергетики и газораспределительных систем	Нарушение условий жизнедеятельности 50 человек и более на 1 сутки и более.
1.3.3.	Аварии на очистных сооружениях	1. Разовое превышение предельно допустимой концентрации (загрязнение) (далее – ПДК) загрязняющего вещества в принимающем сточные воды водном объекте в 50 раз и более. 2. Нарушение условий жизнедеятельности 50 человек и более на 1 сутки и более. 3. Разовое превышение ПДК загрязняющего вещества в атмосферном воздухе за границами санитарно-защитной зоны в 50 раз и более; или в 30-49 раз в течение 8 часов; или в 20-29 раз в течение 2 суток.
1.4.	Аварии с выбросом, сбросом опасных химических веществ	
1.4.1.	Аварии на транспорте с выбросом, разливом, рассыпанием, сбросом опасных химических веществ	1. Разовое превышение загрязнения почвы с превышением ПДК в 5 раз и более. 2. Разовое превышение ПДК опасного химического вещества в водном объекте: 1-2 класса опасности в 5 раз и более; 3-4 класса опасности в 50 раз и более. 3. Разовое превышение ПДК загрязняющего вещества в атмосферном воздухе в 50 раз и более; или в 30-49 раз в течение 8 часов; или в 20-29 раз в течение 2 суток.
1.4.2.	Аварии с выбросом, сбросом опасных химических веществ при производстве, переработке или хранении (захоронении, в том числе в водном объекте)	1. Разрушение сооружений и (или) технических устройств, применяемых на опасном производственном объекте, неконтролируемый взрыв и (или) выброс, сброс опасных химических веществ, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или нарушены условия жизнедеятельности 50 человек и более; или произошло разовое загрязнения почвы с превышением ПДК в 5 раз и более; или произошло разовое превышение ПДК опасного химического вещества в водном объекте: 1-2 класса опасности в 5 раз и более; 3-4 класса опасности в 50 раз и более. 2. Разовое превышение ПДК загрязняющего вещества в атмосферном воздухе в 50 раз и более; или

		в 30-49 раз в течение 8 часов; или в 20-29 раз в течение 2 суток.
1.4.3.	Аварии с боевыми отравляющими веществами	Любой факт аварии.
1.5.	Аварии с разливом (выбросом) нефти, нефтепродуктов	
1.5.1.	Аварии с разливом (выбросом) нефти (нефтепродуктов) на объектах геологического изучения, разведки и добычи углеводородного сырья, а также для переработки производства, транспортировки, хранения, реализации углеводородного сырья и произведенной из него продукции	1. Разлив (выброс) нефти (нефтепродуктов) на сухопутной части территории в объеме 5 т и более. 2. Загрязнение водного объекта (внутренние морские воды, территориальное море, прилежащая и исключительная экономическая зона Российской Федерации, а также поверхностные и подземные водные объекты) нефтью (нефтепродуктами) в объеме 1 т и более. 3. Загрязнение водного объекта источника питьевого водоснабжения в границах 1 и (или) 2 и (или) 3 поясов зоны санитарной охраны.
1.6.	Радиационная авария с выбросом, сбросом, проливом, просыпом ядерных материалов, радиоактивных веществ и радиоактивных отходов	
1.6.1.	Аварии на объектах использования атомной энергии с выбросом радиоактивных веществ (за исключением промплощадок объектов использования атомной энергии и территорий с существующим радиоактивным загрязнением за счет прошлой деятельности и аварий со статусом "зона отчуждения")	1. Прогнозируемые уровни (предполагаемая доза) облучения населения при аварии за короткий срок (2 суток) превышают уровни на[9]: все тело - 1 Гр; легкие - 6 Гр; кожу - 3 Гр; щитовидную железу - 5 Гр; хрусталик глаза - 2 Гр; гонады - 3 Гр; плод - 0,1 Гр. 2. При хроническом облучении, если годовые поглощенные дозы превышают значения на: гонады - 0,2 Гр; хрусталик глаза - 0,1 Гр; красный костный мозг - 0,4 Гр. 3. Критерии для принятия неотложных решений по укрытию населения в начальный период аварии: предотвращаемая доза облучения за первые 10 суток превышает 50 мГр на все тело или 500 мГр на щитовидную железу, легкие, кожу. 4. 100 мкЗв/ч - мощность амбиентного эквивалента дозы на расстоянии 1 м от поверхности земли в среднем по территории.

		5. Объявление состояния "Аварийная обстановка" в соответствии с требованиями федеральных норм и правил в области использования атомной энергии.
1.6.2.	Загрязнение (возможное загрязнение) открытых источников водоснабжения (за исключением технических водоемов объектов использования атомной энергии и водоемов с существующим радиоактивным загрязнением за счет прошлой деятельности и аварий), обусловленное выбросом/сбросом радиоактивных веществ	1. Более 50 УВ (уровень вмешательства) при отсутствии альтернативных источников водоснабжения. 2. Более 100 УВ при наличии альтернативных источников водоснабжения. Критерий относится к долговременному загрязнению (прогнозирование отсутствия значимых снижений активности в водоеме за счет распада радионуклидов и водного стока в течение года) малопроточных и непроточных открытых водоемов, имеющих водохозяйственное значение, а также к водотокам, впадающим в такие водоемы.
1.6.3.	Радиологические аварийные ситуации с источниками ионизирующего излучения и при транспортировке радиоактивных веществ	A/D>1000, где A - активность n-го радионуклида закрытого радионуклидного источника, D - значение величины для n-го радионуклида, являющейся нормирующим фактором, использующимся для разделения широкого диапазона активностей закрытого радионуклидного источника различного радионуклидного состава с целью ранжирования закрытого радионуклидного источника путем отнесения их к одной из категорий опасности.
1.7.	Аварии с выбросом (проливом, просыпом) патогенных для человека микроорганизмов	
1.7.1.	Аварии с выбросом (проливом, просыпом) патогенных для человека микроорганизмов на предприятиях, транспорте и в научно-исследовательских учреждениях (лабораториях)	Любой факт выброса (сброса) веществ, содержащих возбудителей инфекционных заболеваний людей I и II групп патогенности и опасных заболеваний животных.

1.8.	Гидродинамические аварии	
1.8.1.	Аварии на гидротехнических сооружениях	Повреждение или разрушение гидротехнического сооружения, повлекшее за собой неконтролируемый сброс воды из поверхностного водного объекта или хранилища жидких отходов, или нарушение производственного процесса, которое возникло при строительстве, капитальном ремонте, эксплуатации, реконструкции, консервации и ликвидации гидротехнического сооружения, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошло разовое превышение ПДК опасного вещества за границами санитарно-защитной зоны водного объекта в 50 раз и более.
2.	**Природные чрезвычайные ситуации**	
2.1.	Опасные геофизические явления	
2.1.1.	Вулканическое извержение	Вулканическое извержение на территории населенного пункта и (или) на потенциально опасном объекте (далее - ПОО) и (или) критически важном объекте (далее - КВО), в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.1.2.	Землетрясение	Сейсмическое событие магнитудой 5 и более по шкале Рихтера на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.2.	Опасные геологические явления	

2.2.1.	Оползни, обвалы, осыпи	Смещение и (или) отрыв масс горных пород на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.2.2.	Карст, суффозия, просадка в лесовых грунтах	Изменение рельефа, почвенного покрова и несущей способности грунтов на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.2.3.	Овражная (плоскостная) эрозия	Размыв грунтов временными водными потоками на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.2.4.	Криогенное пучение и растрескивание, термокарст, курумы	Изменение почвенного покрова на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или

		произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.	Опасные метеорологические явления	
На основании указанных критериев учреждениями Федеральной службы по гидрометеорологии и мониторингу окружающей среды могут разрабатываться региональные перечни и критерии по обслуживаемым ими территориям с учетом природно-климатических особенностей.		
2.3.1.	Очень сильный ветер, ураганный ветер, шквал, смерч	Ветер при достижении скорости (при порывах) не менее 25 м/с или средней скорости не менее 20 м/с; на побережьях морей и в горных районах при достижении скорости (не при порывах) не менее 30 м/с, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.2.	Очень сильный дождь (мокрый снег, дождь со снегом)	Значительные жидкие или смешанные осадки (дождь, ливневый дождь, дождь со снегом, мокрый снег) с количеством выпавших осадков не менее 50 мм (в селеопасных горных районах - 30 мм) за период времени не более 12 часов, в результате которых: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.3.	Сильный ливень	Количество осадков 30 мм и более за 1 час и менее, в результате которых: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или

		произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.4.	Продолжительный сильный дождь	Дождь с количеством осадков 100 мм и более (в селеопасных горных районах с количеством осадков 60 мм и более) за период времени 48 часов и менее или 120 мм и более за период времени 48 часов и более, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.5.	Очень сильный снег (снегопад)	Снег (снегопад) с количеством 20 мм и более за период времени 12 часов и менее, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.6.	Сильный мороз	В период с ноября по март значение минимальной температуры воздуха достигает установленного для данной территории опасного значения или ниже его, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.7.	Сильная жара	В период с мая по август значение максимальной температуры воздуха достигает установленного для данной территории опасного значения или выше его, в результате которого:

		погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.8.	Крупный град	Град диаметром 20 мм и более, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.9.	Сильная метель	Перенос снега с подстилающей поверхности, часто сопровождаемый выпадением снега из облаков, сильным ветром (со средней скоростью не менее 15 м/с) и с метеорологической дальностью видимости не более 500 м продолжительностью 12 часов и более, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.10.	Сильная пыльная (песчаная) буря	Перенос пыли (песка) сильным ветром (со средней скоростью не менее 15 м/с) и с метеорологической дальностью видимости не более 500 м продолжительностью 12 часов и более, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или

		произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.11.	Сильное гололедно-изморозевое отложение	Отложение на проводах гололедного станка гололеда диаметром 20 мм и более или сложное отложение или мокрый (замерзающий) снег диаметром 35 мм и более или изморозь диаметром 50 мм и более, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.12.	Сильный туман	Сильное помутнение воздуха за счет скопления мельчайших частиц воды (пыли, продуктов горения), с метеорологической дальностью видимости не более 50 м продолжительностью 12 часов и более.
2.3.13.	Заморозки	Понижение температуры воздуха и (или) поверхности почвы (травостоя) до значений ниже 0°С на фоне положительных средних суточных температур воздуха в периоды активной вегетации сельскохозяйственных культур или уборки урожая, приводящее к повреждению и (или) частичной гибели урожая сельскохозяйственных культур на площади 100 га и более.
2.3.14.	Засуха атмосферная	В период вегетации сельскохозяйственных культур отсутствие эффективных осадков (более 5 мм в сутки) за период не менее 30 дней подряд при максимальной температуре воздуха выше 25°С. В отдельные дни (не более 25% продолжительности периода) возможно наличие максимальных температур ниже указанных пределов, в результате чего произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.15.	Засуха почвенная	В период вегетации сельскохозяйственных культур за период не менее 3 декад подряд запасы продуктивной влаги в слое почвы 0-20 см составляют не более 10 мм или за период не менее 20 дней, если в начале периода засухи запасы продуктивной влаги в слое 0-100 см были менее 50 мм, в результате чего произошла гибель посевов

		сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.16.	Сход снежных лавин	Сход снежной лавины, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.3.17.	Комплекс неблагоприятных явлений	Сочетание двух и более одновременно наблюдающихся метеорологических (гидрометеорологических) явлений, каждое из которых в отдельности по интенсивности или силе не достигает критерия опасного явления, но близко к нему, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.4.	Морские опасные гидрометеорологические явления	
2.4.1.	Цунами	Долгопериодные морские гравитационные волны, возникшие вследствие подводных землетрясений, извержений подводных вулканов, подводных и береговых обвалов и оползней, приведших к затоплению прибрежных населенных пунктов, береговых сооружений и народнохозяйственных объектов, в результате которых: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.4.2.	Очень сильный ветер, ураганный ветер (ураган)	Ветер при достижении скорости на акватории океанов, арктических, дальневосточных и антарктических морей (включая порывы) не менее 30 м/с, на акватории других морей - не менее 25 м/с, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или

		имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.4.3.	Сгонно-нагонные явления	Уровни воды ниже опасных отметок с прекращением судоходства, гибелью рыбы, повреждением судов или выше опасных отметок, при которых произошло затопление населенных пунктов, береговых сооружений и объектов, в результате чего: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.4.4.	Сильное волнение	Высота волн в прибрежных районах не менее 4 м, в открытом море не менее 6 м, в открытом океане не менее 8 м, в результате которых: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.5.	Опасные гидрологические явления	
2.5.1.	Высокие уровни воды (половодье, зажор, затор, дождевой паводок)	Подъем уровня воды, в результате которого на территории населенного пункта и (или) на ПОО и (или) КВО: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.

2.5.2.	Низкие уровни воды (низкая межень)	Понижение уровня воды ниже проектных отметок водозаборных сооружений и навигационных уровней на судоходных реках в течение 10 дней и более.
2.5.3.	Раннее ледообразование	Появление льда и образование ледостава (даты) на судоходных реках, озерах и водохранилищах в конкретных пунктах в ранние сроки повторяемостью не чаще 1 раза в 10 лет.
2.5.4.	Сель	Стремительный поток большой разрушительной силы, состоящий из смеси воды и рыхлообломочных пород, внезапно возникающий в бассейнах небольших горных рек вследствие интенсивных дождей или бурного таяния снега, а также прорыва завалов и морен на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.5.5.	Абразия	Размыв и разрушение горных пород в береговой зоне морей на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.5.6.	Речная эрозия	Размыв и смыв грунтов водными потоками на территории населенного пункта и (или) на ПОО и (или) КВО, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или

		произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.6.	Опасные явления в лесах	
2.6.1.	Лесные пожары и другие ландшафтные (природные) пожары	Не локализованы крупные лесные пожары и другие ландшафтные (природные) пожары (площадью 25 га и более в зоне наземной охраны лесов и 200 га и более в зоне авиационной охраны лесов), действующие более 3 суток с момента обнаружения, в отношении которых в установленном порядке не принималось решение о прекращении или приостановке работ по тушению лесного пожара и другого ландшафтного (природного) пожара и (или) более 5 суток действуют нелокализованные лесные пожары и другие ландшафтные (природные) пожары, находящиеся в пределах 5-километровой зоны вокруг населенного пункта или объекта инфраструктуры, и (или) на тушение пожаров привлечено более 50% лесопожарных формирований, пожарной техники и оборудования, предусмотренных планом тушения пожаров соответствующих лесничеств, и резерва, предусмотренного сводным планом тушения лесных пожаров субъекта Российской Федерации.
2.6.2.	Очаги вредителей леса	1. Факт интенсивного распространения очагов вредителей леса на площади 100 га и более, в малолесных субъектах Российской Федерации на площади 10 га и более. 2. Угроза гибели лесных насаждений без проведения своевременных мероприятий по ликвидации очагов вредных организмов, которые осуществляются в ограниченный период, связанный с биологическими особенностями вредителей леса и погодными условиями. 3. Гибель лесных насаждений от воздействия очагов вредителей леса на площади 100 га и более, в малолесных субъектах Российской Федерации на площади 10 га и более.
2.7.	Гелиогеофизические явления	
2.7.1.	Сильное возмущение ионосферы с нарушением коротковолновой связи	Появление и сохранение в течение 3 часов подряд и более отрицательных отклонений максимальных применимых частот при ионосферном распространении радиоволн на величину более 50% от медианных (средних) значений критических частот ($ДF_0F_2$ >50%) или

		полное поглощение сигналов в коротковолновом диапазоне в течение 1 часа и более в полярных областях.
2.7.2.	Сильное возмущение радиационной обстановки в околоземном космическом пространстве	Измеренный в полярных областях на орбитах космических аппаратов высотой более 1000 км поток высокоэнергичных (с энергией $E_p \geq$ 30 МэВ) протонов не менее 800 част./(кв. см х с). Расчетная максимальная мощность дозы проникающих излучений на орбите космических аппаратов высотой 300-500 км и наклонением 52° за защитой 1 г/кв. см алюминия ($P_{мах}$) >25 рад./сут. при магнитной буре, характеризуемой индексами геомагнитной возмущенности $K_p > 5$ или $A_p > 30$.
2.8.	Космические опасности	
2.8.1.	Астероидно-кометная опасность	Поражающее воздействие космических тел на населенный пункт и (или) на ПОО и (или) КВО и окружающую среду, в результате которого: погиб 1 человек и более; или получили вред здоровью 5 человек и более; или имеются разрушения зданий и сооружений; или нарушены условия жизнедеятельности 50 человек и более; или произошла гибель посевов сельскохозяйственных культур и (или) природной растительности на площади 100 га и более.
2.9.	Биологическая опасность	
Отнесение события к чрезвычайной ситуации, связанной с биологической опасностью, осуществляется на основании предложений Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор), Федеральной службы по ветеринарному и фитосанитарному надзору (Россельхознадзор), их территориальных органов и органов государственного ветеринарного надзора и контроля субъектов Российской Федерации в пределах компетенции.		
2.9.1.	Наличие внутренних и внешних опасных биологических факторов, способных привести к возникновению и (или) распространению заболеваний с развитием эпидемий, массовых отравлений, превышению допустимого уровня причинения вреда (с учетом его тяжести) здоровью человека.	
2.9.2.	Наличие внутренних и внешних опасных биологических факторов, способных привести к возникновению и (или) распространению заболеваний с развитием эпизоотии, превышению допустимого уровня причинения вреда сельскохозяйственным животным.	
2.9.3.	Наличие внутренних и внешних опасных биологических факторов, способных привести к возникновению и (или) распространению заболеваний с развитием	

	эпифитотий, превышению допустимого уровня причинения вреда растениям и (или) окружающей среде.

Из вышеперечисленных источников ЧС пояснений могут потребовать следующие виды (частично определения даны по ГОСТ 20.0.03-97, с 1 июля 2023 года заменен на ГОСТ 22.0.03-2022):

Гидродинамическая авария означает чрезвычайное событие, связанное с выходом из строя (разрушением) гидротехнического сооружения или его части, и неуправляемым перемещением больших масс воды, несущих разрушения и затопления обширных территорий.

Абразия – размыв и разрушение горных пород в береговой зоне морей на защищаемой территории.

Эрозия (*речная*) – размыв и смыв грунтов водными потоками на защищаемой территории.

Суффозия – процесс выноса некоторых компонентов грунта (мелкие твердые частицы, растворимые соли) подземными водам.

Ввиду многообразия природных источников ЧС, неопределенности их временной и пространственной локализации, информационные технологии могут помочь на каждом этапе: в предсказании, мониторинге, оперативной и правильной характеризации ЧС, корректного определение ущерба, организации ликвидации последствий и т.д. Необходимость активного развития соответствующих информационных средств и средств поддержки принятия решений подчеркивается статьей 28 Федерального закона от 21.12.1994 № 68-ФЗ (ред. от 14.04.2023) «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», устанавливающей ответственность вплоть до уголовной для должностных лиц, виновных в невыполнении или недобросовестном выполнении законодательства Российской Федерации в области защиты населения и территорий от чрезвычайных ситуаций, непринятии мер по защите жизни и сохранению здоровья людей и других противоправных действиях должностных лиц, что включает и случае несвоевременного предупреждения населения об угрозе ЧС.

Следует еще раз заметить, что вместо ГОСТ 22.0.06-97 с 1 февраля 2024 года вводится в действие в качестве национального стандарта Российской Федерации Межгосударственный стандарт ГОСТ 22.0.06-2023 «Безопасность в чрезвычайных ситуациях. Источники природных чрезвычайных ситуаций. Поражающие факторы. Номенклатура параметров поражающих воздействий»

(введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 июля 2023 г. № 533-ст) [1].

Контрольные вопросы

1. Перечислите четыре основных категории чрезвычайных ситуаций.
2. Какие ЧС относятся к категории техногенных ЧС?
3. Какие шесть видов ЧС относятся к категории природных ЧС?
4. Какие ЧС относятся к категории биолого-социальных? Какие из них несут социальные последствия?
5. Может ли наступивший мороз на территории быть основанием для отнесения ситуаций к разряду чрезвычайных?
6. Может ли массовая гибель рыб считаться основанием для отнесения к разряду ЧС? На основании каких данных или критериев?
7. Что такое курумы и чем они опасны?
8. Чем отличается абразия от эрозии? На каких видах водоемов может происходить каждый из этих видов ЧС?
9. Может ли туман быть источником ЧС? При каких условиях?
10. Какие виды ЧС могут случиться на территории Красноярского края (либо другого конкретного региона)? Какие маловероятны?
11. Какой действующий ГОСТ определяет номенклатуру параметров поражающих воздействий источников ЧС? Какой ГОСТ приходит ему на смену? В чем их отличия?
12. Для каждой из следующих описываемых ситуаций определить:
    а) Есть ли признаки ЧС в этой ситуации?
    б) Если да, то какого характера?
    в) Какая стадия ЧС?
    г) Каков режим функционирования органов РСЧС?

12.1 В пределах городского поселения из-за размытия дорожного покрытия сохраняется риск проседания асфальта. Ранее в это месте уже проваливался грузовик.

12.2 Вдоль берега крупной реки обнаружены разлив нефтепродуктов, в размере 20 кв. м.

12.3 В населенном пункте обнаружены подтопления подвальных помещений жилого сектора. В общей сложности сообщается о подтоплении 4 домов.

12.4 После многоснежной зимы существует опасность паводка в период весеннего половодья на территории со стихийными свалками твердых бытовых и иных отходов.

1. ОСНОВНЫЕ ИСПОЛЬЗУЕМЫЕ В МЧС РОССИИ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1.1 Понятие информационной системы

Под *информационной системой* понимается комплекс, который включает в себя инфраструктуру, организацию, персонал и компоненты, участвующие в сборе, обработке (изменении, обновлении), хранении, передаче, демонстрации и распространении информации [8].

Сбор, обработка, обмен и выдача информации в области защиты населения и территорий от чрезвычайных ситуаций в Единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) осуществляется на основании Федерального закона «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [7].

Положение «О Единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» [9] определяет порядок организации и функционирования Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС). Согласно положению, Единая система объединяет органы управления, силы и средства федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций, в полномочия которых входит решение вопросов по защите населения и территорий от чрезвычайных ситуаций, в том числе по обеспечению безопасности людей на водных объектах, и осуществляет свою деятельность в целях выполнения задач, предусмотренных Федеральным законом «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [7].

Для понимания процессов взаимодействия необходимо знать содержание следующих понятий:

Постоянно действующими органами управления Единой системы являются:

- *на федеральном уровне* – Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также образованные для решения задач в области защиты населения и территорий от чрезвычайных ситуаций подразделения федеральных органов исполнительной власти и государственных корпораций;
- *на межрегиональном уровне* – территориальные органы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным

ситуациям и ликвидации последствий стихийных бедствий, расположенные в субъектах Российской Федерации, в которых находятся центры соответствующих федеральных округов;

- *на региональном уровне* – территориальные органы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- *на муниципальном уровне* – создаваемые при органах местного самоуправления органы, специально уполномоченные на решение задач в области защиты населения и территорий от чрезвычайных ситуаций;
- *на объектовом уровне* – структурные подразделения организаций, специально уполномоченные на решение задач в области защиты населения и территорий от чрезвычайных ситуаций.

Органами повседневного управления Единой системы являются:

- *на федеральном уровне* – Национальный центр управления в кризисных ситуациях Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также организации (подразделения), обеспечивающие деятельность федеральных органов исполнительной власти и государственных корпораций в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и привлекаемыми для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях;
- *на межрегиональном уровне* – центры управления в кризисных ситуациях территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, расположенных в субъектах Российской Федерации, в которых находятся центры соответствующих федеральных округов, а также организации (подразделения) территориальных органов федеральных органов исполнительной власти межрегионального уровня, обеспечивающие деятельность этих органов в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и привлекаемыми для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях на межрегиональном уровне;

- *на региональном уровне* – центры управления в кризисных ситуациях территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также организации (подразделения) территориальных органов федеральных органов исполнительной власти по субъектам Российской Федерации и организации (подразделения) органов исполнительной власти субъектов Российской Федерации, обеспечивающие деятельность этих органов в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и привлекаемыми для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях;
- *на муниципальном уровне* – единые дежурно-диспетчерские службы муниципальных образований, подведомственные органам местного самоуправления, дежурно-диспетчерские службы экстренных оперативных служб, а также другие организации (подразделения), обеспечивающие деятельность органов местного самоуправления в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и привлекаемыми для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях;
- *на объектовом уровне* – подразделения организаций, обеспечивающие их деятельность в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и привлекаемыми для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях.

На данный момент существует широкий спектр информационных систем, разработанных и успешно применяемых в повседневной работе органов управления РСЧС. Эти системы различаются по типу и включают *информационно-справочные системы*, *геоинформационные системы*, *аналитические системы, модели развития сценариев ЧС, системы поддержки принятия решений*. Согласно анализу, проведенному НЦУКС [10], в органах повседневного управления уже на 2017 год насчитывалось порядка 600 информационных систем РСЧС, представляющих интерес в области защиты

населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

Сравнительный анализ используемых в работе МЧС России специализированных информационных систем рассмотрен, в частности, в статье [11]. В работе выявлено, например, что некоторые из них дублируют друг друга своими функциональными возможностями и инструментарием. Широкий спектр информационных систем используется для мониторинга и прогнозирования чрезвычайных ситуаций. К таким информационным системам, например (см. [11]), относятся:

- информационно-аналитическая система «ИАС ДТП»;
- система дистанционного мониторинга «Каскад»;
- система дистанционного мониторинга лесных пожаров «ИСДМ Рослесхоз»;
- система видео мониторинга лесопожарной обстановки «Лесной дозор»;
- система видео мониторинга лесопожарной обстановки «Лесохранитель»;
- система управления силами и средствами Всероссийской службы медицины катастроф «ФБД СиС ВСМК»;
- автоматизированный программно-технический комплекс по планированию и организации мероприятий гражданской обороны «АПТК-ГО»;
- автоматизированный программно-технический комплекс «Безопасный город»;
- автоматизированная информационная система государственного мониторинга водных объектов «АИС ГМВО»;
- модуль картографического интерфейса отраслевой системы мониторинга водных биологических ресурсов, наблюдения и контроля за деятельностью промысловых судов «МКИ ОСМ»;
- единая государственная система информации об обстановке в Мировом океане «ЕСИМО»;
- комплексная интегрированная система обеспечения мониторинга и государственного управления на морском и внутреннем водном транспорте «КИИС МОРЕ»;
- система «Поиск-Море»;
- система «ОБОРОНЛЕС»;

- автоматизированная система контроля радиационной обстановки «АСКРО Росатом»;
- единая государственная автоматизированная система мониторинга радиационной обстановки «ЕГАСМРО»;
- система мониторинга судов «СМС Виктория»; система по водным ресурсам и водному хозяйству бассейнов рек России «ГисВодИнфо»;
- информационная система «Ясень»;
- информационная система «ЕСВИТМ-Туристы»;
- система информационного обеспечения «ПАК БРИЗ»;
- «СПО ЦМП СЗРЦ»;
- программный комплекс «Пожароопасность»;
- автоматизированная система информационного обеспечения СМПЧС и НЦУКС;
- информационная система «Магистраль»;
- информационная система «Лесные пожары»;
- программный комплекс «Волна»; автоматизированная система информационного обеспечения СМПЧС и НЦУКС;
- программа «Оценка последствий лесных пожаров» и т.д.

Также, наиболее важные информационные системы кратко описаны в статьях [12] и [11], мы будем следовать аналогичному описанию.

1.2 Классификация информационных систем

В органах повседневного управления МЧС России используется порядка 100 информационных систем, которые можно разделить на три части:

- информационные системы МЧС России (таблица 1.1);
- информационные системы федеральных органов исполнительной власти (таблица 1.2);
- международные информационные системы (таблица 1.3).

Далее, в таблицах 1.1-1.3, приводится перечень основных информационных систем с краткой характеристикой органа или ведомства ответственного за эту систему и перечнем информации, используемой в деятельности органов повседневного управления МЧС России.

Таблица 1.1 – Перечень и краткие характеристики основных информационных систем МЧС России, используемых в органах повседневного управления МЧС России.

Наименования системы	Краткое описание основных функциональных возможностей системы	Информация, необходимая для оперативной диспетчерской службы органов повседневного управления МЧС России
АИС ГИМС (Автоматизированная система ГИМС МЧС России) (www.gims.ru)	Предназначена для обеспечения ведения Единого реестра зарегистрированных маломерных судов и государственного учета выдаваемых удостоверений на право управления маломерными судами, регистрационных и иных документов, необходимых для допуска маломерных судов и судоводителей к участию в плавании. Учет зарегистрированных маломерных судов. Учет удостоверений судоводителей	Единый реестр зарегистрированных маломерных судов
СтатГИБДД (http://stat.gibdd.ru/)	Показатели состояния безопасности дорожного движения	Система предназначена для информационно-статистического обеспечения
Термические точки	Приложение создано с целью ликвидации возгораний в природной среде в кратчайшие сроки и минимизации риска перехода огня на населенные пункты. Позволяет сократить время доведения до сил РСЧС информации об очагах горения, получаемой посредством космического мониторинга.	Учет термических точек и анализ возможной угрозы населенным пунктам
ПК ДАР (Программный комплекс динамического анализа рисков)	Предназначен для выполнения расчетов показателей рисков от совместного воздействия природных, техногенных и биолого-социальных опасностей на основе статистических данных, построения карт риска от природных, техногенных и биологических опасностей на территории РФ.	Показатели рисков следующих опасностей: землетрясения, наводнения, пожары, метеорологические опасности, геологические опасности, взрывы, пожары, аварии с выбросом опасных химических веществ, аварии на транспорте. Карты рисков от природных, техногенных и биологических опасностей на территории РФ

Продолжение таблицы 1.1.

СМТС СВОД Глонасс	Контроль состояния и местоположения транспортных средств и принятие решений по управлению ими на основе полученной информации	Точные данные о местоположении транспортных средств в режиме реального времени с использованием навигационной аппаратуры системы ГЛОНАСС/GPS
СМИС (Структурированная система мониторинга и управления инженерными системами зданий и сооружений) (smis-expert.com)	Мониторинг систем инженерно-технического обеспечения, состояния оснований строительных конструкций зданий и сооружений, технологических процессов, сооружений инженерной защиты и передача в режиме реального времени информации об угрозе и возникновении чрезвычайных ситуаций, в том числе вызванных террористическими актами, по каналам связи в ОПУ РСЧС	Параметры технологических и инженерных систем объектов, критически важных для безопасности людей, находящихся в них, и в окружающей среде. Информация об инцидентах, авариях, пожарах, террористических проявлениях на объекте
АПТК-ГО (Аппаратно-программный комплекс гражданской обороны)	Ведение баз данных объектов, имущества и сил гражданской обороны, оценка параметров возможной обстановки в военное время и при возникновении чрезвычайных ситуаций техногенного характера, решение аналитических задач по гражданской обороне, а также для формирования и ведения планирующих документов	Базы данных объектов, имущества и сил гражданской обороны, оценка параметров обстановки в военное время и при ЧС техногенного характера, решение аналитических задач по ГО, планирующих документов в области ГО
КСМ-ЗН (Комплексная система мониторинга состояния защиты населения на радиоактивно загрязненных территориях)	Мониторинг в автоматизированном режиме ключевых параметров радиационной обстановки на федеральном уровне, раннее предупреждение о возникновении ЧС с радиационным фактором; прогноз развития ЧС с радиационным фактором, своевременное предупреждение населения и информационная поддержка деятельности территориальных и федеральных органов исполнительной власти по обеспечению радиационной безопасности на контролируемой территории. Входит в Единую государственную автоматизированную систему контроля радиационной обстановки (ЕГАСКРО)	Данные датчиков радиационного мониторинга. Радиационные расчетные задачи

Окончание таблицы 1.1.

Единая интегрированная система ведения данных по рискам на туристических маршрутах	Эксплуатация сотрудниками Центров управления в кризисных ситуациях МЧС России, осуществляющих контроль рисков возникновения и развития ЧС на туристических маршрутах	Моделирование возможного развития чрезвычайной ситуации на туристических маршрутах и объектах туристической инфраструктуры. Статистическая информация по туристическим маршрутам
Геопортал «Экстремум» (gis.extremum.org)	Своевременное выявление зон с показателями индивидуального риска, превышающими допустимые значения, а также планирование превентивных мероприятий по защите территорий субъектов РФ, муниципальных образований, критически важных объектов экономики и обеспечение поддержки принятия решений при оперативном реагировании в ЧС	Моделирование природных и техногенных ЧС
СКМ МЧС России (Система космического мониторинга МЧС России)	Обеспечение органов управления РСЧС федерального и территориального уровней оперативной информацией о состоянии территорий, находящихся в зонах повышенного риска возникновения ЧС, фактах возникновения ЧС, параметрах обстановки в районах ЧС и динамики ее дальнейшего развития	Результаты космического мониторинга паводков, пожаров, сейсмических событий
АС НЦУКС (Автоматизированная система Национального центра управления в кризисных ситуациях)	Информационное обеспечение ОДС НЦУКС, ЦУКС территориальных органов МЧС России и других пользователей МЧС России	Данные о чрезвычайных ситуациях и происшествиях, природных пожарах (по данным о проверенных и непроверенных термоточках из СКМ); туристических группах на туристических маршрутах, радиационной обстановке из автоматизированной системы КСМ-ЗН, информация сводного реестра по аварийно-спасательным формированиям, информация об объектах транспортной инфраструктуры, промышленности и социально важных объектах

Таблица 1.2 – Перечень и краткие характеристики основных информационных систем федеральных органов исполнительной власти (ФОИВ), используемых в органах повседневного управления МЧС России

Наименования системы и ФОИВ	Основное функциональное назначение системы	Информация, необходимая для оперативной диспетчерской службы органов повседневного управления МЧС России
Федеральная база данных «*Силы и средства медицины катастроф Минздрава России*». Минздрав России, Федеральный центр медицины катастроф ФГБУ «НМХЦ им. Пирогова» Миздрава России (sis.minzdrav.gov.ru)	Получение общей информации о медицинских учреждениях	Силы и средства медицинских учреждений (места дислокации, возможности, оснащенность). Возможности медицинских учреждений. Оперативная информация по ЧС, на которые выезжают силы Минздрава России
ЕГАСМРО. Росгидромет. НПО Тайфун (www.vmm310.ru)	Государственный мониторинг радиационной обстановки на территории России	Оперативная информация о радиационной обстановке
СИМО. Росгидромет (http://esimo.ru/portal)	Обеспечение федеральных органов исполнительной власти аналитической, прогностической и обобщенной информацией о состоянии морской среды и морской деятельности, полученной в результате наблюдений	Сведения о системах наблюдений за океаном в России и за рубежом, организациях экспертах, платформах морской деятельности (судах, портах и др.). Сведения об информационных ресурсах ведомственных информационных систем. Справочные сведения о состоянии морской среды и морской деятельности. Электронные картографические материалы
АИСДМ-Рослесхоз. ФБУ «Авиалесоохрана» (aviales.ru)	Мониторинговая система предназначена для получения ежедневных отчетов, карт горимости, данных космического мониторинга	Термоточки на территории России. Космические снимки очагов пожара. Оперативные и статистические данные по очагам пожара, данные о силах и средствах пожаротушения. Карты горимости
АИС ГМВО Автоматизированная информационная система государственного мониторинга водных объектов. Росводресурсы (gmvo.skniivh.ru)	Информационное обеспечение управления водными ресурсами, государственного контроля и надзора за использованием и охраной водных объектов	Состояние поверхностных вод, дна, берегов, водоохранных зон, подземных вод, водохозяйственных систем, в том числе ГТС. Данные контроля и надзора. Нормативные требования к водному объекту

Окончание таблицы 1.2.

Комплексная интегрированная информационная система «*МоРе*» Информационный аналитико-статистический центр Росморречфлота (portal.shipsea.ru)	Интеграция информационных ресурсов в области безопасности судоходства, мониторинга, учета и классификации судов	Обеспечение оперативной и интегрированной информацией о морском и речном транспорте заинтересованных федеральных органов исполнительной власти и организаций. Обеспечение участия Российской Федерации в поддержании существующих и создании новых международных и региональных систем контроля за судоходством. Обеспечение комплексного контроля за судоходством за счет обработки данных.
ПК ЦУП. Минтранс России Федеральное дорожное агентство – Росавтодор (www.pkcup.ru)	Комплексный контроль и анализ ситуаций на сети автомобильных дорог, принятие решений по ее содержанию и предупреждению участников дорожного движения	Сервис объективного контроля за метеообстановкой на федеральных трассах. Оперативная фотоинформации.
ГИС-портал Ситуационно-Аналитического Центра Минэнерго России. Минэнерго России (сацминэнерго.рф)	Мониторинг пожарной и метеорологической обстановки на объектах ТЭК	Данные о трубопроводах, ЛЭП, подстанциях, пунктах диспетчерского управления, месторождениях, перерабатывающих заводах и др.
«*СИРАНО*». Федеральная служба по ветеринарному и фитосанитарному надзору – Россельхознадзор (portal.eskigov.ru/fgis/323)	Быстрое и удобное оповещение служб в целях обеспечения эффективности мер ветеринарного надзора и контроля	Сведения о заболеваниях животных
Служба срочных донесений. Единая геофизическая служба Российской академии наук (http://www.gsras.ru/new/ssd_news.htm)	Сейсмический мониторинг	Данные по произошедшим землетрясениям с описанием их характеристик и нанесением на картографическую основу. Данные по сейсмологическим станциям мира
ЕМИСС. Федеральная служба государственной статистики – единая межведомственная информационно-статистическая система (fedstat.ru)	Ведение официальной статистической информации, формируемой субъектами официального статистического учета	Статистические данные, из ведомственных хранилищ данных

Таблица 1.3 – Перечень и краткие характеристики основных международных информационных систем, используемых в органах повседневного управления МЧС России

Наименования системы и организации	Основное назначение системы	Информация, необходимая для органов повседневного управления МЧС России
GDACS (Global Disaster Alert and Coordination System). Организация объединенных наций и Европейская комиссия (www.gdacs.org)	Координация в процессе глобальных катастроф	Информация о сейсмособытиях, тропических циклонах, наводнениях, вулканических извержениях, засухе и лесных пожарах в мире
RSOE EDIS (Emergency and Disaster Information Service). Национальная ассоциация инфокоммуникаций (www.rsoe-edis.org)	Информирование о катастрофах в мире	Данные по чрезвычайным ситуациям и катастрофам в мире с отображением на картографической основе
CSEM EMSC. Европейский средиземноморский сейсмологический центр (www.emsc-csem.org)	Сейсмический мониторинг в Средиземноморье	Интерактивная карта сейсмособытий. Подробная характеристика произошедших землетрясений
JTWC. Центр наблюдения за тайфунами	Мониторинг воздушных масс в мире	Информация по движениям воздушных масс, циклонам, треки движения, скорость ветра в мире
Marinetraffic. Открытый ресурс (www.marinetraffic.com)	Наблюдение за положением судов в мире	Информация по движениям судов, краткая информация по судам, фото судов в мире
Flightradar24.Открытый ресурс (www.flightradar24.com)	Мониторинг воздушных судов	Местоположение и треки воздушных судов в мире
NASA FIRMS Web Fire Mapper. Национальное управление по воздухоплаванию и исследованию космического пространства США (firms.modaps.eosdis.nasa.gov)	Мониторинг природных пожаров в мире	Карта активных точек горения, архив пожаров в мире
HealthMap. Открытый ресурс (www.healthmap.org/ru/)	Мониторинг эпидемиологической обстановки на Земле	Карта инфекций, заболеваний людей и животных
SeaLevel. ЮНЕСКО (ioc-sealevelmonitoring.org)	Мониторинг уровня моря в мире	Данные уровня моря мониторинга в мире
NukeMap. Открытый ресурс (nuclearsecrecy.com/nukemap)	Моделирование возможных последствий ядерного взрыва для всего мира	Зоны избыточного давления, поражающей радиации, распространения радиоактивных осадков, приблизительное количество пострадавших и погибших

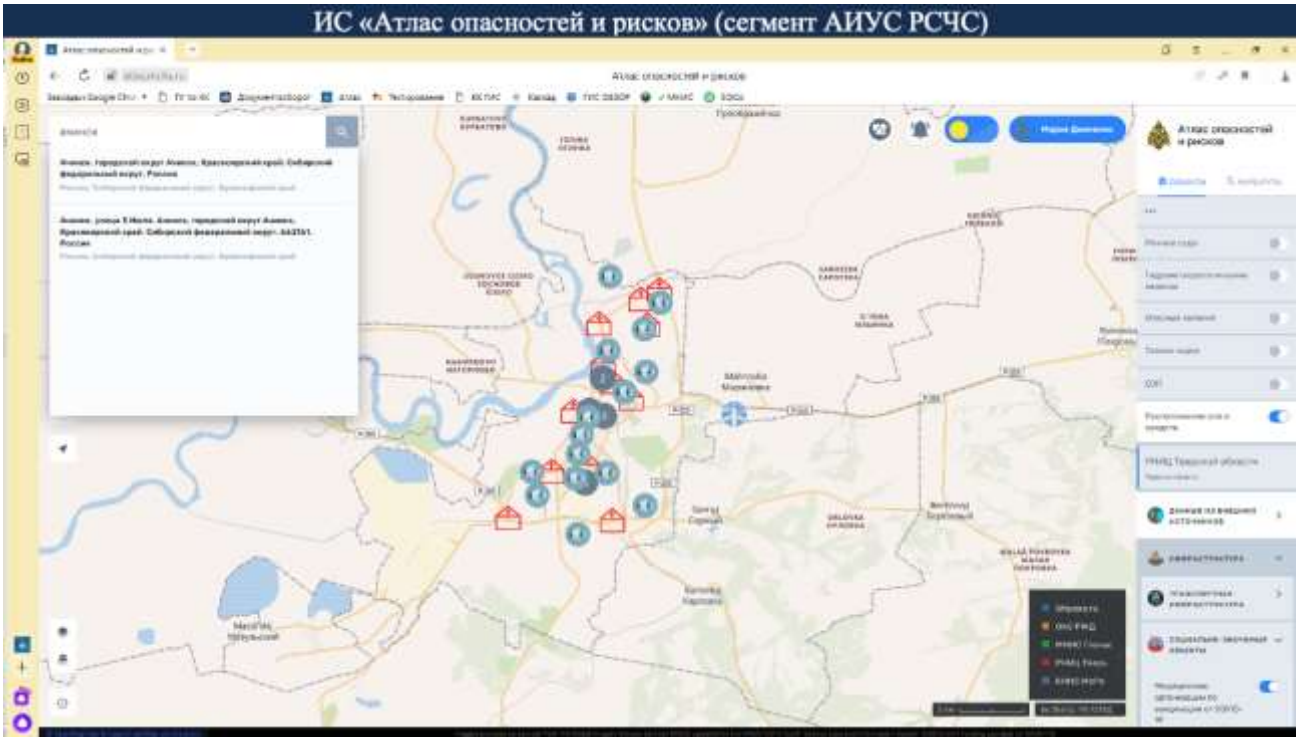

Рисунок 1.1. – Атлас опасностей и рисков МЧС России.
(Источник: https://atlas.mchs.gov.ru/)

Рисунок 1.2. – Геоинформационная система «КАСКАД».

1.3 Контрольные вопросы

1. Что такое информационная системы?
2. Какая система в МЧС России осуществляет сбор, обработку, обмен и выдача информации в области защиты населения и территорий от чрезвычайных ситуаций?
3. Какие органы системы РСЧС являются постоянно действующими органами управления?
4. Какие органы системы РСЧС являются органами повседневного управления?
5. К каким трем типам можно отнести информационные системы, разработанные и применяемые в повседневной работе органов управления РСЧС?
6. Приведите примеры информационных систем МЧС России.
7. Приведите примеры международных информационных систем.
8. Приведите примеры федеральных органов исполнительной власти.
9. Какая система служит для оповещений о цунами?

2. АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩАЯ СИСТЕМА (АИУС) ЕДИНОЙ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Автоматизированная информационно-управляющая система РСЧС (*АИУС РСЧС*) – это система сбора, комплексной обработки оперативной информации о чрезвычайных ситуациях и информационного обмена между различными подсистемами и звеньями РСЧС, передачи органами повседневного управления необходимых указаний силам и средствам ликвидации чрезвычайных ситуаций. В автоматическом режиме система способна выполнять задачи сбора, хранения, передачи, обработки и выдачи информации, необходимой для обеспечения работы органов управления РСЧС, автоматизации процессов поддержки принятия управленческих решений, доведения принятых решений до подчиненных и взаимодействующих органов управления и контроля их исполнения. В составе системы имеются следующие основные средства:

- комплекс средств автоматизации (КСА), размещаемых на стационарных пунктах управления;
- мобильные КСА подвижных пунктов управления; абонентские комплекты пользователей;
- КСА взаимодействия с внешними по отношению к МЧС России структурами;
- сеть связи и передачи данных.

На базе перечисленной техники создаются объектовые комплексы средств автоматизации АИУС (см. [8]).

АИУС РСЧС имеет аналогичную организационную структуру, как и РСЧС. Более того, АИУС РСЧС является функциональной системой, охватывающей всю территорию Российской Федерации и все уровни РСЧС. Она предназначена для автоматизации широкого спектра задач. За время его создания и развития было протестировано множество подходов, разработано и внедрено множество решений, связанных с АИУС РСЧС.

Из-за масштабности и сложности задач РСЧС требуется разделение АИУС РСЧС на отдельные взаимосвязанные компоненты, которые могут создаваться и развиваться независимо. Эти компоненты включают ведомственные и территориальные решения, такие как мобильное приложение «Термические точки» и другие. Логичным и естественным шагом в данном контексте является

внедрение и постепенный переход к единой интеграционной платформе, которая обеспечит необходимую основу для решения отдельных задач в рамках АИУС РСЧС. Переход на единую интеграционную платформу предусматривает переходный период, в течение которого обеспечивается функционирование самой платформы и ее ресурсов, а также программно-технических решений, разработанных до внедрения единой интеграционной платформы. К концу переходного периода все используемые ресурсы АИУС РСЧС должны быть адаптированы для работы в рамках единого программно-технического комплекса на основе единой интеграционной платформы АИУС РСЧС.

На момент написания данного учебного пособия Государственная информационная система АИУС РСЧС создается на базе информационной системы «Атлас опасностей и рисков», причем в целях определения правового статуса разработана концепция ГИС АИУС РСЧС и определены некоторые основные понятия, рассматриваемые ниже, которые находятся в стадии принятия.

2.1 Основные понятия АИУС РСЧС

Рассмотрим основные понятия и определения.

«*Автоматизированная информационно-управляющая система*» единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (*АИУС РСЧС*) – государственная информационная система, представляющая собой совокупность программных и технических средств, средств связи, оповещения, автоматизации, информационных ресурсов и баз данных, обеспечивающая обмен данными, подготовку, сбор, хранение, обработку, анализ и передачу информации в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

Доступ к информации, содержащейся в АИУС РСЧС – возможность получения информации из АИУС РСЧС и ее использования в соответствии с законодательством Российской Федерации.

Личный кабинет пользователя – инструмент обмена информацией в области защиты населения и территорий от чрезвычайных ситуаций между пользователями АИУС РСЧС.

Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций – система, объединяющая органы управления, силы и средства федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных корпораций и организаций, в полномочия которых входит

решение вопросов по защите населения и территорий от чрезвычайных ситуаций, в том числе по обеспечению безопасности людей на водных объектах.

Информация в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера – информация, содержащаяся в АИУС РСЧС, о прогнозируемых и возникших чрезвычайных ситуациях природного и техногенного характера и их последствиях, мерах по защите населения и территорий, ведении аварийно-спасательных и других неотложных работ, силах и средствах, задействованных для ликвидации чрезвычайных ситуаций природного и техногенного характера, радиационной, химической, медико-биологической, взрывной, пожарной и экологической безопасности на соответствующих объектах и территориях, а также о деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных корпораций и организаций в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, составе и структуре сил и средств, предназначенных для предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера, в том числе сил постоянной готовности, их создании и наличии, об использовании и о восполнении финансовых и материальных ресурсов для ликвидации чрезвычайных ситуаций природного и техногенного характера.

Органы управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций – органы, создаваемые для координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных корпораций и организаций в области защиты населения и территорий от чрезвычайных ситуаций и сил, привлекаемых для предупреждения и ликвидации чрезвычайных ситуаций.

2.2 Цели и задачи АИУС РСЧС

Целью создания АИУС РСЧС является информационное обеспечение и развитие системы управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС), как части системы государственного управления, с использованием инновационных технологий и цифровизации процессов поддержки принятия решения при предупреждении и ликвидации последствий чрезвычайных ситуаций (ЧС).

Основные задачи АИУС РСЧС:

- обеспечение информационного взаимодействия участников АИУС РСЧС в цифровом формате (сбор, учет, хранение, обработка, анализ, а также предоставление информации, содержащейся в АИУС РСЧС) для решения вопросов по защите населения и территорий от ЧС;
- осуществление мер информационной поддержки органов управления РСЧС для принятия решений в области защиты населения и территорий от ЧС.

2.3 Структура, функции и принципы функционирования АИУС РСЧС

В составе АИУС РСЧС функционируют два взаимосвязанных контура: *закрытый*, функционирующий в защищенной сети связи, и *открытый*, функционирующий в сети «Интернет».

Закрытый контур АИУС РСЧС представлен следующими структурными элементами:

- геоинформационная система;
- база знаний;
- блок аналитики;
- блок работы с данными дистанционного зондирования Земли;
- информационно-аналитическая система.

Открытый контур АИУС РСЧС реализован в виде сайта в сети «Интернет» и *личного кабинета пользователя*. *Личный кабинет пользователя* состоит из следующих блоков:

- блок Атлас опасностей и рисков (https://atlas.mchs.gov.ru/);
- блок Паспорт территорий (https://cabinet.mchs.gov.ru/);
- блок Термические точки (https://firenotification.mchs.gov.ru/);
- блок Информационно-аналитическая система (https://edds.mchs.gov.ru/);
- блок Мобильное приложение Термические точки МЧС.

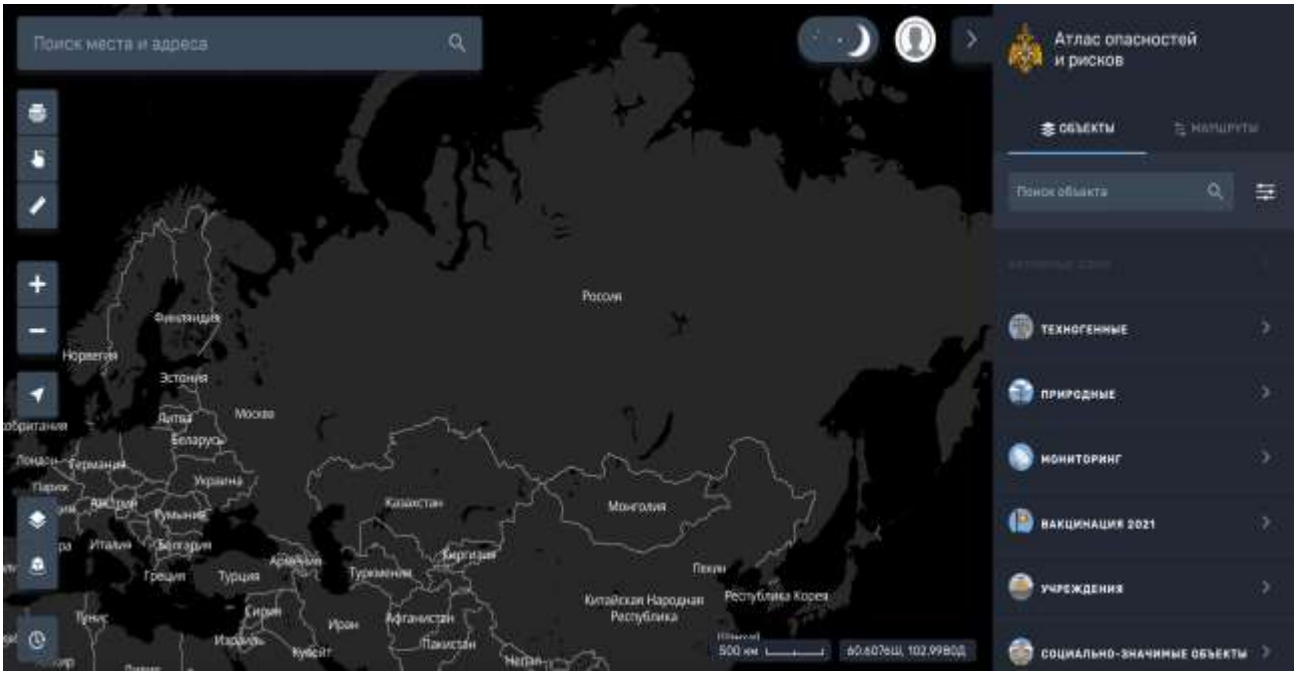

Рисунок 2.1. – Атлас опасностей и рисков.
(Источник: https://atlas.mchs.gov.ru/)

Закрытый контур АИУС РСЧС обеспечивает возможность выполнения следующих функций:

- сбор, хранение, обмен и визуализация оперативной и плановой информации;
- ввод, поиск и хранение структурированных и неструктурированных текстовых и медиаданных;
- проведение расчетов возможных последствий ЧС с использованием расчетных модулей, разработанных на основе национальных стандартов Российской Федерации, методик и научно-методических подходов, утвержденных федеральными органами исполнительной власти по направлениям деятельности;
- проведение исследований данных, проверок гипотез и эффективности разрабатываемых аналитических подходов и получаемых результатов.

Открытый контур АИУС РСЧС на основе личного кабинета пользователя обеспечивает возможность выполнения следующих функций:

- осуществление геопространственного анализа;
- обеспечение информационного взаимодействия с закрытой частью АИУС РСЧС; доведение до пользователей АИУС РСЧС ежедневного

оперативного прогноза возникновения ЧС и результатов расчетов возможных последствий ЧС;

- оперативное доведение до пользователей АИУС РСЧС информации о термических точках.

В АИУС РСЧС могут создаваться иные подсистемы (блоки), необходимые для решения ее задач.

2.4 Участники АИУС РСЧС

Участниками АИУС РСЧС являются:

- оператор АИУС РСЧС;
- *поставщики информации* – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, государственные корпорации и организации, которые передают информацию в области защиты населения и территорий от ЧС в АИУС РСЧС;
- *пользователи информации* – федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, государственные корпорации и организации, а также юридические и физические лица, использующие систему в целях получения информации и принятия решений вопросов в области защиты населения и территорий от ЧС.

Оператор АИУС РСЧС обеспечивает:

- создание, ввод в эксплуатацию, эксплуатацию и развитие АИУС РСЧС;
- координацию взаимодействия участников АИУС РСЧС;
- разработку единых механизмов передачи и получения данных для взаимодействия с поставщиками и пользователями АИУС РСЧС;
- методическую и консультационную поддержку участников АИУС РСЧС по вопросам ее использования;
- защиту информации, содержащейся в АИУС РСЧС, в том числе целостность и доступность обрабатываемой в ней информации;
- разграничение прав доступа участников АИУС РСЧС к информации, содержащейся в АИУС РСЧС;

- информационное взаимодействие АИУС РСЧС с другими информационными системами, содержащими информацию в области защиты населения и территорий от ЧС.

Поставщики информации:

- обладают доступом к информации, содержащейся в АИУС РСЧС;
- передают в АИУС РСЧС информацию в области защиты населения и территорий от ЧС;
- обеспечивают целостность, достоверность и установленную степень конфиденциальности информации, подлежащей передаче в АИУС РСЧС;
- незамедлительно информируют оператора АИУС РСЧС о сбоях и нарушениях в работе АИУС РСЧС, а также о нарушениях требований к обеспечению информационной безопасности, о возникновении технических проблем, связанных с предоставлением информации для включения в АИУС РСЧС, о сроках их устранения, об изменении действующих форматов данных и о порядке предоставления информации, содержащейся в АИУС РСЧС (получения доступа к ней).

Пользователи АИУС РСЧС:

- имеют доступ к информации, содержащейся в АИУС РСЧС;
- принимают управленческие решения в области защиты населения и территорий от ЧС, предупреждения и ликвидации ЧС, в том числе на основе анализа данных и результатов расчетов возможных последствий ЧС;
- имеют право распространять общедоступную информацию, содержащуюся в АИУС РСЧС, при условии указания в качестве источника распространения такой информации оператора АИУС РСЧС.

2.5 Порядок предоставления информации для включения в АИУС РСЧС и предоставления содержащейся в ней информации (получения доступа к ней)

В АИУС РСЧС размещается следующая информация.

- Информация в области защиты населения и территорий от ЧС:
  - сведения о прогнозируемых и возникших ЧС природного и техногенного характера и их последствиях;

- сведения о мерах по защите населения и территорий от ЧС, ведении аварийно-спасательных и других неотложных работ, силах и средствах, задействованных для ликвидации ЧС, радиационной, химической, медико-биологической, взрывной, пожарной и экологической безопасности на соответствующих объектах и территориях;
- сведения о деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, государственных корпораций и организаций в области защиты населения и территорий от ЧС;
- сведения о составе и структуре сил и средств, предназначенных и задействованных для ликвидации ЧС, в том числе сил постоянной готовности;
- сведения о создании, наличии, использовании и восполнении финансовых и материальных ресурсов для ликвидации ЧС;

- данные об объектах инфраструктуры (объекты социальной, транспортной, инженерной, производственной, торговой, экономической, туристской инфраструктуры и др.);
- данные дистанционного зондирования Земли и результаты их обработки;
- статистическая, в том числе официальная, информация и нормативная справочная информация, которая может быть использована в области защиты населения и территорий от ЧС.

Размещению в АИУС РСЧС не подлежит информация и документы, содержащие сведения, составляющие государственную тайну в соответствии с законодательством Российской Федерации о государственной тайне.

Поставщики информации несут ответственность за полноту, достоверность и своевременность размещения в АИУС РСЧС электронных документов и информации в соответствии с требованиями законодательства Российской Федерации.

При использовании информации, содержащейся в АИУС РСЧС, пользователь информации обязан указывать АИУС РСЧС в качестве источника этой информации, а также обладателей (поставщиков) такой информации.

2.6 Порядок информационного взаимодействия АИУС РСЧС с иными информационными системами

Информационное взаимодействие АИУС РСЧС с иными информационными системами осуществляется в соответствии с законодательством Российской Федерации и (или) соглашениями и регламентами (протоколами) информационного обмена.

При организации информационного взаимодействия АИУС РСЧС и иных информационных систем может быть использована единая система межведомственного электронного взаимодействия.

При организации информационного взаимодействия АИУС РСЧС и иных информационных систем должны быть выполнены требования законодательных и иных нормативных правовых актов Российской Федерации в области защиты информации, не составляющей государственную тайну, а также должны использоваться технические средства защиты информации, сертифицированные Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в части, касающейся средств криптографической защиты информации.

Организация информационного взаимодействия АИУС РСЧС с иными информационными системами осуществляется оператором АИУС РСЧС и операторами иных информационных систем самостоятельно или с привлечением организаций, находящихся в их ведении, или иных организаций в соответствии с законодательством Российской Федерации в области контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд.

2.7 Контрольные вопросы

1. Дайте определение АИУС РСЧС.
2. Дайте определение основной цели создания АИУС РСЧС.
3. Перечислите основные задачи АИУС РСЧС.
4. Какие структурные элементы входят в закрытый контур АИУС РСЧС?
5. Какие блоки входят в открытый контур АИУС РСЧС?
6. Кто является участниками АИУС РСЧС?
7. Какая информация размещается в АИУС РСЧС?
8. Опишите порядок информационного взаимодействия АИУС РСЧС с иными информационными системами.

3. СИСТЕМЫ МОНИТОРИНГА

3.1 Общие понятия о мониторинге окружающей среды и прогнозировании ЧС

В России разработана система для мониторинга и прогнозирования различных опасностей и угроз природного и техногенного характера. Эта система основана на комплексном подходе к сбору и обработке данных, с целью обеспечить оперативное обнаружение широкого спектра возможных угроз. Основное внимание уделяется созданию эффективных аналитических систем и сервисов, которые наблюдают за предвестниками стихийных бедствий и контролируют состояние опасных объектов. Ниже рисунок 3.1 показывает основные цели мониторинга согласно [13].

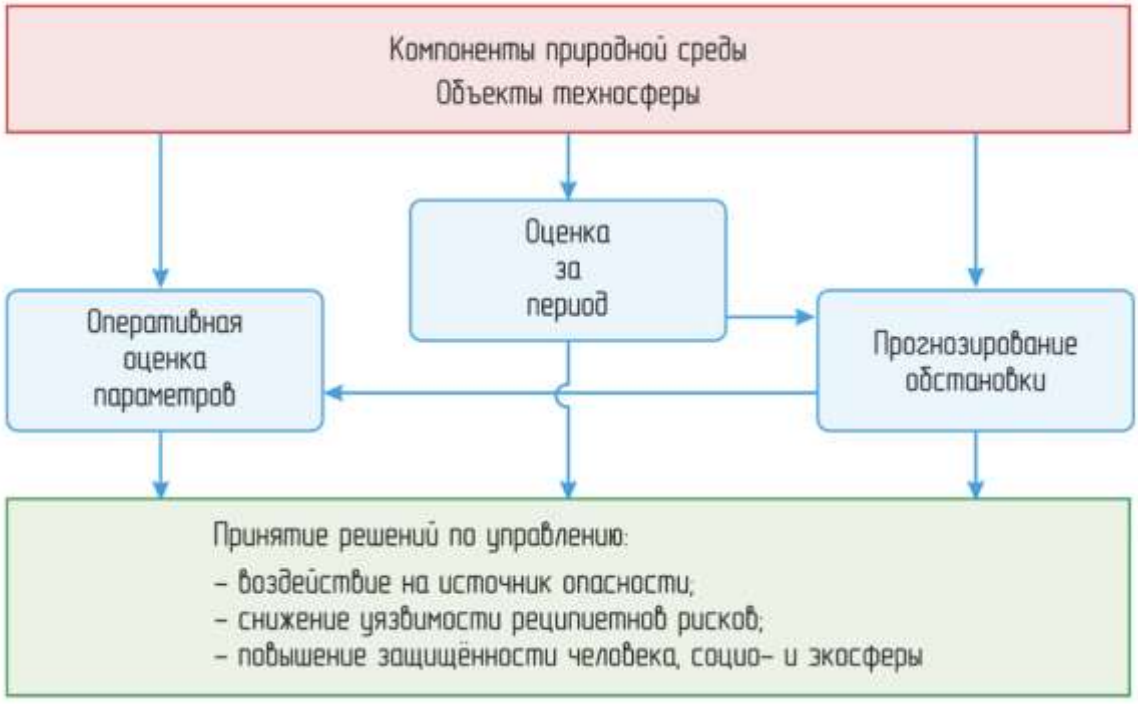

Рисунок 3.1. – Цели мониторинга.

Рассмотрим общие понятия о мониторинге окружающей среды и прогнозировании ЧС соответственно ГОСТ Р 22.1.02-95 [14].

Мониторинг – система наблюдений и контроля, проводимых регулярно, по определенной программе для оценки состояния окружающей среды, анализа происходящих в ней процессов и своевременного выявления тенденций ее изменения.

Прогнозирование чрезвычайных ситуаций; прогнозирование ЧС – опережающее отражение вероятности возникновения и развития чрезвычайной

ситуации на основе анализа возможных причин ее возникновения, ее источника в прошлом и настоящем.

Прогнозирование может носить *долгосрочный*, *краткосрочный* или *оперативный* характер.

Объект мониторинга – природный, техногенный или природно-техногенный объект, или его часть, в пределах которого по определенной программе осуществляются регулярные наблюдения за окружающей средой с целью контроля за ее состоянием, анализа происходящих в ней процессов, выполняемых для своевременного выявления и прогнозирования их изменений и оценки.

Также, документ [14] включает в себя понятия по мониторингу и прогнозированию опасных природных процессов и явлений:

- мониторинг опасных природных процессов и явлений;
- прогнозирование опасных геологических процессов и явлений;
- прогнозирование опасных атмосферных процессов и явлений;
- прогнозирование опасных гидрологических процессов и явлений;
- прогнозирование природных пожаров.

В частности, *прогнозирование природных пожаров* – это определение вероятности возникновения и динамики развития природных пожаров с оценкой вероятных неблагоприятных последствий.

В зависимости от масштаба ЧС, различают пять уровней (ступеней) мониторинга:

- *глобальный* (биосферный) мониторинг – предусматривает слежение за общемировыми процессами и явлениями в биосфере и осуществление прогноза возможных изменений;
- *национальный* осуществляется в пределах государства специально созданными органами;
- *региональный* охватывает отдельные регионы, в пределах которых имеют место процессы и явления, отличающиеся по природному характеру или по антропогенным воздействиям от общего базового фона;
- *местный* мониторинг на уровне сообществ;
- *локальный* мониторинг предусматривает осуществление наблюдений в особо опасных зонах и местах, обычно непосредственно примыкающих к источникам загрязняющих веществ.

Каждый нижеследующий уровень мониторинга входит составной частью в вышеперечисленный уровень.

Отметим, что документ [14] устанавливает требования к нормативному обеспечению мониторинга окружающей среды и прогнозирования ЧС, а также требования к метрологическому обеспечению мониторинга и прогнозирования ЧС.

Системы мониторинга могут условно подразделяться по различным признакам (см. [13]):

- пространственному охвату;
- объекту наблюдения (абиотическая компонента: атмосферный воздух, воды суши и морей, почвы, геологическая среда; биотическая компонента: растительный и животный мир, живая природа на охраняемых природных территориях, человек; физические факторы воздействия: ионизирующее излучение, электромагнитное излучение, тепловое излучение, шумы, вибрация);
- методам (прямое инструментальное измерение, дистанционная съемка, косвенная индикация, опросы, дневниковые наблюдения);
- степени отношения эффекта и процесса, за которыми ведутся наблюдения;
- типу воздействия (геофизическое, биологическое, медико- географическое, социально-экономическое, общественное);
- целям (определение современного состояния среды, исследование явлений, оценка и градуировка моделей окружающей среды, краткосрочный прогноз, долгосрочные выводы, оптимизация и повышение экономической эффективности исследований и прогнозов, контроль за воздействием на среду и т.д.).

Мониторинг безопасности различных типов и уровней подробно рассмотрен в монографии [13]. В основе организации систем мониторинга учитываются общие теоретические и методологические принципы:

1. *Структурно-организационный принцип* – система мониторинга любого уровня, являясь многоуровневой иерархической структурой, должна строиться с учетом взаимодействия с высшими системами и низшими подсистемами.
2. *Функциональный принцип* – мониторинг функционирует во времени как взаимосвязанная и взаимообусловленная система цепи постоянных наблюдений, оценки, прогноза и управления.

3. *Обучающий принцип* – с течением времени в системе работающего мониторинга качество прогнозов и эффективность управления должны закономерно улучшаться, система мониторинга во времени должна непрерывно совершенствоваться и строиться как «самообучающаяся» система.
4. *Пространственный принцип* – пространственная структура системы пунктов получения информации формируется в зависимости от вида мониторинга и определяется природными геологическими и инженерно-геологическими особенностями территории, типом и особенностями инженерных сооружений на ней, а также состоянием на ней экосистемы.
5. *Временной принцип* – частота наблюдений и сбора информации во времени в системе мониторинга полностью определяется динамикой наблюдаемых (изучаемых) процессов.
6. *Целевой принцип* – система любого мониторинга должна строиться с учетом достижения его конечной цели – оптимизации управления, что достигается на базе прогнозных оценок ее развития путем выработки оптимальных управляющих решений и рекомендаций.

3.2 Нормативное обеспечение мониторинга

Выделим нормативные акты, которые регулируют деятельность различных сфер мониторинга в Российской Федерации. Эти акты включают законы, постановления, приказы и рекомендации.

3.2.1 Метеорологический и гидрологический мониторинг

- Федеральный закон от 19 июля 1998 г. № 113-ФЗ «О гидрометеорологической службе».
- Постановление Правительства РФ от 23.07.2004 № 372 (ред. от 09.03.2022) «О Федеральной службе по гидрометеорологии и мониторингу окружающей среды».
- Постановление Правительства РФ от 06.06.2013 № 477 (ред. от 03.08.2020) «Об осуществлении государственного мониторинга состояния и загрязнения окружающей среды».
- Постановление Правительства РФ от 15 ноября 1997 г. № 1425 «Об информационных услугах в области гидрометеорологии и мониторинга загрязнения окружающей природной среды».

- Постановление Правительства РФ от 16.11.2020 № 1845 (ред. от 28.02.2022) «О лицензировании деятельности в области гидрометеорологии и смежных с ней областях (за исключением указанной деятельности, осуществляемой в ходе инженерных изысканий, выполняемых для подготовки проектной документации, строительства, реконструкции объектов капитального строительства)» (вместе с «Положением о лицензировании деятельности в области гидрометеорологии и смежных с ней областях (за исключением указанной деятельности, осуществляемой в ходе инженерных изысканий, выполняемых для подготовки проектной документации, строительства, реконструкции объектов капитального строительства)»).
- «Водный кодекс Российской Федерации» от 03.06.2006 № 74-ФЗ.
- Приказ Федеральной службы по гидрометеорологии и мониторингу окружающей среды от 13 июля 2021 г. № 218 «Об утверждении Перечня работ федерального назначения в области гидрометеорологии и смежных с ней областях».

3.2.2 Экологический мониторинг

- Федеральный закон «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ.
- Федеральный закон «Об охране атмосферного воздуха» от 04.05.1999 N 96-ФЗ.
- Постановление Правительства РФ от 9 августа 2013 г. № 681 «О государственном экологическом мониторинге (государственном мониторинге окружающей среды) и государственном фонде данных государственного экологического мониторинга (государственного мониторинга окружающей среды)».
- Постановление Правительства РФ от 15 ноября 1997 г. № 1425 «Об информационных услугах в области гидрометеорологии и мониторинга загрязнения окружающей природной среды».
- Постановление Правительства РФ от 28.03.2008 № 214 «О внесении изменений в Положение об информационных услугах в области гидрометеорологии и мониторинга загрязнения окружающей природной среды».

3.2.3 Санитарно-эпидемический мониторинг

- Федеральный закон «О санитарно-эпидемиологическом благополучии населения» от 30.03.1999 № 52-ФЗ.

3.2.4 Радиационный мониторинг

- Федеральный закон «О радиационной безопасности населения» от 09.01.1996 № 3-ФЗ.
- Санитарные правила и нормативы СанПиН 2.6.1.2523-09 «Нормы радиационной безопасности НРБ-99/2009» (утв. постановлением Главного государственного санитарного врача РФ от 7 июля 2009 г. № 47).

3.2.5 Лесопожарный мониторинг

- «Лесной кодекс Российской Федерации» от 04.12.2006 № 200-ФЗ

3.2.6 Мониторинг функционирования потенциально опасных объектов

- Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ.
- СНиП 2.06.01-86 Гидротехнические сооружения. Основные положения проектирования.

3.3 Организация гидрологического мониторинга

Гидрометцентр России отвечает за прогнозирование потенциально опасных явлений по всей стране. Это включает прогнозирование метеорологических условий и осадков. Региональные центры используют региональные модели и наблюдения, чтобы уточнить размеры опасных зон. Территориальные центры используют численные методы для оценки вероятности возникновения явлений. Оперативные прогностические подразделения уточняют прогноз, учитывая текущую ситуацию на основе данных спутников, радиолокаторов и собранных наблюдений.

Главной задачей всех прогностических подразделений является предоставление прогнозов и предупреждений о возможных опасных явлениях с максимально возможной заблаговременностью. Опасные гидрометеорологические явления включают такие, которые могут представлять угрозу для безопасности людей и нанести значительный ущерб экономике. Эти явления оцениваются как опасные, когда достигают критических значений гидрометеорологических величин.

На основе длительных наблюдений выделяются области, подверженные наводнениям. В этих областях проводится наблюдение за паводковой ситуацией. С использованием данных Росгидромета отслеживается уровень воды в реках на гидропостах. На основе этих данных, а также прогноза погоды на короткий и

долгий срок, анализируется рельеф местности в информационных системах МЧС России для создания моделей развития паводков. Чтобы объективно оценить характер и последствия моделирования, проводится трехмерная визуализация. Автоматически рассчитываются последствия наводнения, определяется количество домов и населения, подверженных возможному затоплению, а также определяются необходимые ресурсы и меры для реагирования и предотвращения чрезвычайных ситуаций. После этого вся информация передается главам муниципальных образований.

На территории России наблюдаются более 20 видов опасных гидрометеорологических явлений, которые регулярно исследуются и прогнозируются. Они включают сильные ветры, шквалы, смерчи, пыльные бури, ливни и грозы, град, сильные дожди, засухи, заморозки, снегопады, метели, гололедно-изморозевые явления, туманы, сильные морозы, наводнения, снежные лавины, сели и другие. Эти явления могут негативно влиять на производственную и хозяйственную деятельность общества.

Федеральный закон «О гидрометеорологической службе» [15] устанавливает правовые основы деятельности в области гидрометеорологии и смежных с ней областях (деятельности гидрометеорологической службы) и направлен на обеспечение потребностей государства, физических и юридических лиц в гидрометеорологической, гелиогеофизической информации, а также в информации о состоянии окружающей среды, ее загрязнении. В частности, в рамках Федерального закона вводятся такие понятия как

- *гидрометеорологическая служба* – система функционально объединенных индивидуальных предпринимателей, юридических лиц, федеральных органов исполнительной власти Российской Федерации, органов исполнительной власти субъектов Российской Федерации и Государственной корпорации по атомной энергии «Росатом», осуществляющих деятельность в области гидрометеорологии и смежных с ней областях (метеорологии, климатологии, агрометеорологии, гидрологии, океанологии, гелиогеофизики, области активных воздействий на гидрометеорологические процессы), мониторинг состояния и загрязнения окружающей среды, в том числе ионосферы и околоземного космического пространства, предоставление информации о состоянии окружающей среды, ее загрязнении, об опасных природных явлениях;
- *мониторинг состояния и загрязнения окружающей среды* – долгосрочные наблюдения за состоянием окружающей среды, ее загрязнением и

происходящими в ней природными явлениями, а также оценка и прогноз состояния окружающей среды, ее загрязнения;

- *стационарный пункт наблюдений* за состоянием окружающей среды, ее загрязнением – комплекс, включающий в себя земельный участок или часть акватории с установленными на них приборами и оборудованием, предназначенными для определения характеристик окружающей среды, ее загрязнения;
- *государственная наблюдательная сеть* – наблюдательная сеть федерального органа исполнительной власти в области гидрометеорологии и смежных с ней областях.

Гидрометеорологическая служба входит в состав единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) и осуществляет свою деятельность в чрезвычайных ситуациях в соответствии с законодательством РФ о защите населения и территорий от ЧС природного и техногенного характера.

Государственная наблюдательная сеть, согласно возложенным на нее задачам, осуществляет [16]:

- проведение регулярных метеорологических, аэрологических, гидрологических, морских гидрометеорологических, агрометеорологических, специальных гидрометеорологических, геофизических и гелиогеофизических наблюдений, а также наблюдений за уровнем загрязнения атмосферного воздуха, почв, поверхностных вод суши и морской среды, атмосферных осадков, снежного покрова, включая радиоактивное загрязнение;
- выполнение наблюдений за опасными гидрометеорологическими, гелиогеофизическими явлениями (ОЯ), высокими и экстремально высокими уровнями загрязнения окружающей среды;
- выполнение первичной обработки результатов всех наблюдений (в том числе анализ проб объектов природной среды);
- передачу в установленном порядке оперативной информации о фактическом состоянии окружающей среды, ее загрязнении, информации об ОЯ, распространение информации общего назначения в соответствии с утвержденным планом и схемой обеспечения;
- обеспечение в установленном порядке органов государственной власти, отраслей экономики, Вооруженных Сил Российской Федерации, а также

населения информацией о фактическом состоянии окружающей среды, ее загрязнении, прогнозами и предупреждениями, получаемыми от прогностических органов Росгидромета.

В состав гидрометеорологической сети входят следующие наблюдательные сети (по видам наблюдений):

- авиаметеорологическая;
- агрометеорологическая;
- актинометрическая (раздел геофизики, изучающий солнечную, земную и атмосферную радиацию);
- аэрологическая (радиозондирование);
- воднобалансовая;
- гелиогеофизическая;
- гидрологическая на болотах;
- гидрологическая на реках и каналах;
- гидрометеорологическая на озерах и водохранилищах;
- гляциологическая;
- ионосферная;
- магнитная;
- метеорологическая;
- метеорологическая радиолокационная (МРЛ);
- морская гидрометеорологическая (в прибрежной зоне, в том числе в устьях рек, и в открытой части морей и океанов, включая морскую судовую и экспедиционную сети);
- селестоковая;
- снеголавинная;
- озонометрическая;
- теплобалансовая.

Кроме того, к гидрометеорологической сети относятся также наблюдательные сети:

- за атмосферным электричеством;
- за испарением с поверхности воды, почвы, снега.

Основная наблюдательная сеть – это часть государственной наблюдательной сети, репрезентативная относительно общего фона климатообразующих и других природных факторов, обеспечивающая

необходимую точность получения фоновых значений гидрометеорологических величин для любой точки территории между пунктами наблюдений. Основная наблюдательная сеть представляет собой минимально необходимую с точки зрения научной, хозяйственной и экономической целесообразности сеть, предназначенную для изучения режима и состояния окружающей среды, ее загрязнения, гидрометеорологического обеспечения страны в целом или крупных ее регионов.

Дополнительная наблюдательная сеть предназначена для решения локальных задач по учету специфичных гидрометеорологических условий и для изучения состояния окружающей среды, ее загрязнения в особых физико-географических и климатических районах.

Стационарный пункт наблюдений за состоянием окружающей среды, ее загрязнением – комплекс, включающий в себя земельный участок или часть акватории с установленными на них приборами и оборудованием, предназначенными для определения характеристик окружающей среды, ее загрязнения. К стационарным пунктам наблюдений относят также специально отведенный земельный участок или выделенную часть акватории без установленных на них приборов и оборудования, где проводятся регулярные определения характеристик окружающей среды, ее загрязнения по отдельным видам наблюдений.

Коротко опишем средства мониторинга, качающиеся опасных гидрологических явлений.

Прогнозы наводнений основываются на комплексе гидрометеорологических характеристик. Эти характеристики учитываются в различных программах для вычисления прогноза и включают в себя предыдущую реакцию водосбора на осадки, уровни воды в реках, дефицит почвенной влаги, информацию о выпадающих осадках, общую синоптическую обстановку, ветер, атмосферное давление и другие гидрометеорологические параметры.

Региональные гидрометцентры занимаются разработкой прогнозов наводнений. Краткосрочные прогнозы паводковых наводнений могут быть предоставлены с заблаговременностью от 1 до 3 суток, а долгосрочные прогнозы половодий могут быть предоставлены с заблаговременностью от 1 до 2,5 месяцев.

К опасным гидрологическим явлениям относятся:

- *высокие уровни воды* (при половодьях, паводках, заторах, зажорах, ветровых нагонах), при которых возможно затопление населенных пунктов и нарушение нормальной деятельности береговых сооружений и объектов;
- *низкие уровни воды* – ниже проектных отметок водозаборных сооружений и предельных навигационных уровней на судоходных реках и водоемах;
- *ранее ледообразование* на судоходных реках и озерах;
- *отрыв льдов в местах выхода людей на лед*;
- *половодье* – ежегодный подъем уровня воды в реках, вызываемый таянием снега и льда до отметок обеспеченностью наивысших уровней менее 10 %;
- *зажор* – скопление масс шуги и внутриводного льда в период осеннего шугохода и в начале ледостава, создающее стеснение русла на отдельном участке реки и вызывающий изменение уровня воды до отметок обеспеченностью менее 10 %;
- *затор* – скопление льда во время ледохода, создающее стеснение русла на отдельном участке реки и вызывающее изменение уровня воды до отметок обеспеченностью менее 10 %;
- *паводок* – быстрый подъем уровня воды, возникающий нерегулярно, от сильных дождей и кратковременного снеготаяния до отметок обеспеченностью наивысших уровней менее 10 %;
- *низкая межень* – понижение уровня воды ниже проектных отметок водозаборных сооружений и предельных навигационных уровней на судоходных реках и озерах в конкретных пунктах в течение не менее 10 дней;
- *ранее ледообразование* – появление льда и образование ледостава (даты) на судоходных реках, озерах и водохранилищах в конкретных пунктах в ранние сроки повторяемостью не чаще 1 раза в 10 лет.

Гидрометеорологические явления, которые по своей интенсивности и продолжительности могут нанести значительный ущерб экономике и представляют угрозу безопасности людей, называют *стихийными гидрометеорологическими явлениями*.

Особое внимание уделяется речным ледовым прогнозам. Разрабатываются программные системы расчета и краткосрочного прогноза основных элементов ледового режима основных рек. При составлении краткосрочных прогнозов за основу берутся метеорологические данные по прогнозу на 5 суток, что и определяет заблаговременность прогноза. Оправдываемость краткосрочных

прогнозов сроков появления льда и вскрытия рек составляет 92-95 %. В основу методики среднесрочных прогнозов положено использование прогноза средней температуры воздуха на декаду с учетом распределения температуры поверхности океана в качестве фона развития процесса. Эта методика позволяет внести уточнения в большинство долгосрочных прогнозов. Долгосрочные прогнозы (с заблаговременностью 1-2 месяца) сроков замерзания и вскрытия рек имеют среднюю оправдываемость около 80%, но она недостаточно устойчива, в связи с чем большое внимание уделяется методам уточнений с заблаговременностью 10-20 суток.

Величина и интенсивность весенне-паводковых наводнений зависят от следующих условий:

- запасов воды в снежном покрове к моменту таяния снега и их распространения по площади водосбора;
- интенсивности снеготаяния, зависящей от метеорологических условий; степени влажности и глубины промерзания почв водосбора до выпадения первого снега осенью;
- площади, рельефа и формы водосбора, наличия озер, болот, лесов, влияющих на условия стекания снеговых вод;
- количества осадков, выпадающих в период таяния снега; образования ледяной корки на почве; сочетания волн половодья крупных притоков бассейна; образования заторов и зажоров льда.

Для гидрологического мониторинга и прогнозирования наводнений применяются три группы методов:

1. *Визуальные наблюдения*: включают наблюдение за осадками, речным стоком, уровнем воды, снежным покровом, влажностью почвы, подземными водами, температурой воды, озерным и речным льдом, испарением.
2. *Инструментальные измерения*: включают использование гидрологических станций, расположенных на реках, озерах, водохранилищах, для измерения уровня воды, расхода и накопления запасов воды.
3. *Аналитические методы*: включают изучение предвестников наводнений и анализ информации, получаемой от системы мониторинга. Использование детерминированных и статистических методов (в том числе, основанные на методах машинного обучения) позволяет делать прогнозы на средне- и долгосрочные периоды.

Для сбора данных гидрометеорологического характера, организации Росгидромета сотрудничает с администрациями субъектов РФ. Также используются данные международной системы гидрометеорологических спутников.

Применение современных моделей для прогнозирования требует мощной вычислительной техники и полной автоматизации процесса получения данных, их контроля, анализа и расчета. Набор объективных методов прогноза погодных элементов и явлений, основанных на численных методах, позволяет делать прогнозы с заблаговременностью 24-36 часов. Комплексные системы слежения за погодой, использующие данные спутников и наземных наблюдений, постоянно уточняют прогнозы и предупреждают о возможных опасных локальных явлениях.

Кроме того, все большее распространение получает космический мониторинг, который позволяет наблюдать за развитием наводнений, оценивать их масштабы и ущерб, а также в ряде случаев предсказывать наводнения. Спутниковые системы позволяют оперативно определить площадь наводнения, найти участки, подверженные затоплению, и планировать защитные и восстановительные операции для сдерживания наводнений. Спутниковые изображения во время наводнений сопоставляются с картами, чтобы измерить площадь затопленных земель.

Для целей дистанционного зондирования из космоса используются космическая система «Метеор», система исследования мирового океана «Океан», система изучения поверхности суши «Ресурс», ряд экспериментальных отечественных аппаратов, а также данные международной системы геостационарных гидрометеорологических спутников США, Японии и европейских спутников METEOSAT.

3.4 Мониторинг природных пожаров

Рассмотрим мониторинг экстремальных состояний экосистем. Согласно [17] рассмотрим основные понятия:

Ландшафтный (природный) пожар – неконтролируемый процесс горения, стихийно возникающий и распространяющийся в природной среде, охватывающий различные компоненты природного ландшафта;

Лесной пожар – разновидность ландшафтного (природного) пожара, распространяющегося по лесу.

Мониторинг пожарной опасности в лесах и лесных пожаров осуществляется, в частности, в соответствии с Лесным кодексом Российской Федерации от 04.12.2006 № 200-ФЗ (ред. от 04.08.2023), Статья 53.2, и включает в себя:

1. наблюдение и контроль за пожарной опасностью в лесах и лесными пожарами;
2. организацию системы обнаружения и учета лесных пожаров, системы наблюдения за их развитием с использованием наземных, авиационных или космических средств;
3. организацию патрулирования лесов;
4. прием и учет сообщений о лесных пожарах, а также оповещение населения и противопожарных служб о пожарной опасности в лесах и лесных пожарах специализированными диспетчерскими службами.

В целях пожарной безопасности в лесах осуществляются следующие мероприятия:

- наблюдение и контроль за пожарной опасностью в лесах и лесными пожарами;
- организацию системы обнаружения и учета лесных пожаров, системы наблюдения за их развитием с использованием наземных, авиационных или космических средств;
- организацию патрулирования лесов;
- прием и учет сообщений о лесных пожарах, а также оповещение населения и противопожарных служб о пожарной опасности в лесах и лесных пожарах специализированными диспетчерскими службами.

Уполномоченные органы исполнительной власти субъектов Российской Федерации, осуществляющие переданные им полномочия в области лесных отношений, представляют в уполномоченный федеральный орган исполнительной власти данные о пожарной опасности в лесах и лесных пожарах.

По результатам мониторинга пожарной опасности в лесах и лесных пожаров уполномоченный федеральный орган исполнительной власти принимает решение о маневрировании лесопожарных формирований, пожарной техники и оборудования в соответствии с межрегиональным планом маневрирования лесопожарных формирований, пожарной техники и оборудования.

Для оценки природной пожарной опасности в лесах обычно применяется метод классификации пожарной опасности, разработанный В.Г. Нестеровым в 1949 году. Этот метод регулируется приказом [18].

Формула расчета *класса природной пожарной опасности* (КПО) в лесах в зависимости от условий погоды определяется как сумма произведения температуры воздуха на разность температур воздуха и точки росы за дни без дождя (считая день выпадения более 3 мм осадков первым днем бездождевого периода). Иными словами, значение коэффициента в i-й день наблюдений можно записать как

$$\text{КПО}_i = \sum_{k=m}^{i} t_k \cdot \left(t_k - t_k^d\right),$$

где

- t_k – температура воздуха в k-й день наблюдений в 12-15 часов ($^\circ C$),
- t_k^d – температура точки росы в k-й день наблюдений в тот же момент времени ($^\circ C$),
- m – максимальное число, меньшее или равное i, такое, что между наблюдениями в (m –1)-й и m-й день выпало более трех мм осадков.

КПО Нестерова начинают рассчитывать с дня, когда на рассматриваемой территории окончательно сходит снежный покров. Общероссийская шкала (Таблица 3.1) имеет пять классов пожарной опасности. Тем не менее, для отдельных регионов границы значений КПО Нестерова для каждого класса могут различаться, более того, известны различные варианты обобщения данного показателя.

Таблица 3.1 – Федеральные классы пожарной опасности в лесах в зависимости от условий погоды

Класс пожарной опасности в лесах	Величина комплексного показателя	Степень пожарной опасности
I	0…300	Отсутствует
II	301…1000	Малая
III	1001…4000	Средняя
IV	4001…10000	Высокая
V	Более 10000	Чрезвычайная

В резервных лесах весь комплекс мероприятий по обеспечению пожарной безопасности выполняется на лесных участках, примыкающих к населенным пунктам и объектам экономики. На остальной территории резервных лесов ведется мониторинг пожарной опасности в лесах в части обнаружения лесных пожаров и наблюдения за их динамикой с использованием преимущественно космических и авиационных средств.

При I классе пожарной опасности в лесах по условиям погоды организуется (см. [19]):

- наземное патрулирование проводится в местах огнеопасных работ в целях контроля за соблюдением правил пожарной безопасности в лесах;
- авиационное патрулирование и дежурство на пожарных наблюдательных пунктах не ведутся.

При II классе пожарной опасности в лесах по условиям погоды организуется:

- наземное патрулирование проводится на лесных участках, отнесенных к I и II классам природной пожарной опасности лесов, а также в местах массового отдыха людей в лесах;
- авиационное патрулирование проводится через 1-2 дня, а при наличии пожаров - ежедневно в порядке разовых полетов;
- дежурство на пожарных наблюдательных пунктах и на пунктах приема донесений о пожарах от экипажей патрульных самолетов и вертолетов осуществляется во время проведения наземного и авиационного патрулирования.

При III классе пожарной опасности в лесах по условиям погоды организуется:

- наземное патрулирование проводится на лесных участках, отнесенных к первым трем классам природной пожарной опасности лесов, а также в местах проведения работ и в местах, наиболее посещаемых населением;
- авиационное патрулирование проводится 1-2 раза в течение дня;
- дежурство на пожарных наблюдательных пунктах и на пунктах приема донесений о пожарах от экипажей патрульных самолетов и вертолетов осуществляется во время проведения наземного и авиационного патрулирования;
- наземные и авиационные пожарные команды, если они не заняты на тушении пожаров, в полном составе находятся на местах дежурства;

- по местным радиотрансляционным сетям и с помощью звукоусилительных установок на самолетах и вертолетах авиационной охраны лесов, особенно в дни отдыха, передаются напоминания о необходимости осторожного обращения с огнем в лесу;
- может ограничиваться разведение костров и посещение отдельных участков лесов.

При IV классе пожарной опасности в лесах по условиям погоды организуется:

- наземное патрулирование проводится с 8 до 21 часа;
- авиационное патрулирование проводится не менее двух раз в день;
- дежурство на пожарных наблюдательных пунктах и на пунктах приема донесений о пожарах от экипажей патрульных самолетов и вертолетов ведется с 9 до 21 часа;
- силы и средства пожаротушения, в том числе резервные, должны находиться в состоянии готовности к тушению пожаров;
- организуется предупреждение населения о высокой пожарной опасности в лесах;
- организуется ежедневное дежурство ответственных лиц с 9 до 24 часов;
- у дорог при въезде в лес устанавливаются щиты, предупреждающие об опасности пожаров в лесах;
- ограничивается посещение отдельных наиболее пожароопасных участков леса (I-III классов природной пожарной опасности лесов), запрещается разведение костров в лесах.

При V классе пожарной опасности в лесах по условиям погоды организуется:

- наземное патрулирование лесов проводится в течение всего светлого времени суток, а в наиболее пожароопасных местах – круглосуточно;
- авиационное патрулирование проводится не менее 3 раз в день;
- дежурство на пожарных наблюдательных пунктах и на пунктах приема донесений о пожарах от экипажей патрульных самолетов и вертолетов ведется с 9 до 21 часа;
- силы и средства пожаротушения, в том числе резервные, должны находиться в состоянии готовности к тушению пожаров;

- противопожарная пропаганда должна быть максимально усилена, передачи напоминаний об осторожном обращении с огнем в лесу по местным ретрансляционным сетям проводятся через каждые 2-3 часа;
- максимально ограничивается въезд в леса средств транспорта, а также посещение леса населением, закрываются имеющиеся на дорогах в лес шлагбаумы, устанавливаются щиты, предупреждающие о чрезвычайной пожарной опасности, выставляются посты на контрольно-пропускных пунктах.

Минприроды России осуществляет информационную поддержку в области обнаружения и тушения лесных пожаров, а также предоставляет информацию и технологии для анализа последствий этих пожаров. Для этого функционирует информационная система дистанционного мониторинга лесных пожаров, известная как *ИСДМ-Рослесхоз*.

Основными задачами, для решения которых используется в ИСДМ-Рослесхоз, являются:

- получение оперативной информации для оценки лесопожарной обстановки на основе метеоданных;
- оперативное обнаружение лесных пожаров, наблюдение за их динамикой и прогноз дальнейшего развития;
- оперативная оценка характеристик действующих пожаров (площадь, направление развития, задымленность и т.д.);
- оценка и уточнение площадей, пройденных огнем;
- комплексный анализ данных об отдельных пожарах, в том числе для проверки информации, предоставляемой региональными диспетчерскими службами;
- получение отчетных форм и статистической информации о лесных пожарах.

Для решения данных задач в ИСДМ-Рослесхоз используются в основном спутниковые данные.

В случае опасности осуществляется информирование населения для населения по средствам СМИ, социальных сетей, операторов сотовой связи, средств ОКСИОН и системы оповещения.

3.5 Использование беспилотных авиационных систем в вопросах мониторинга

Большую роль в мониторинге играют беспилотные летательные аппараты. На базе высших учебных заведений МЧС России реализуются программы по обучению и повышению квалификации внешних пилотов беспилотных авиационных систем (БАС). Ниже дан краткий обзор основных понятий, используемых для применения беспилотных авиационных систем в МЧС России.

Мероприятия по производству полетов беспилотных воздушных систем организовываются в соответствии с требованиями Воздушного законодательства Российской Федерации, документов, регламентирующих деятельность государственной авиации и нормативных документов МЧС России в части, касающихся БАС.

Основные цели применения беспилотных авиационных систем в МЧС России это:

- организованное, правомерное и безопасное использование (применение) стоящих на оснащении БАС, сил и средств управления ими;
- сбор, обработка и доведение до заинтересованных лиц получаемой с помощью БВС информации для принятия грамотных управленческих решений в ходе выполнения задач по предупреждению ЧС и ликвидации их последствий, выполнению аварийно-спасательных, поисково-спасательных и других неотложных работ.

Рисунок 3.2. – Применение беспилотной авиации в деятельности МЧС России.

Основные цели управления подразделениями беспилотной авиации МЧС России:

- *в повседневном режиме* – поддержание постоянной готовности подразделений беспилотной авиации к действиям по предназначению;
- *при ЧС* – подготовка и выполнение с применением БАС разведывательных, специальных и транспортных задач в интересах МЧС России.

Основные задачи, стоящие перед подразделениями беспилотной авиации МЧС России перечислены ниже:

- *разведывательные:*
  - ведение воздушной разведки с целью доведения в масштабе времени близком к реальному до органов управления и сил МЧС России необходимой информации;
  - ведение длительного мониторинга пожароопасной, паводковой и ледовой обстановки;
  - воздушный поиск объектов заинтересованности, воздушное патрулирование заданных районов, контроль надводной обстановки;
  - воздушная разведка очагов природных и техногенных пожаров;
  - воздушная разведка зон подтопления;
  - контроль зон ЧС, определение границ района ЧС и точных координат объектов поиска;
  - воздушная разведка путей выдвижения оперативных групп и спасательных подразделений, определение путей эвакуации населения и пострадавших из зоны ЧС;
  - разведка погоды;
  - сопровождение, наведение и корректировка действий спасательных подразделений и мобильных поисковых групп;
  - ведение поисковых авиационных работ на водных акваториях, в лесных массивах, труднодоступных районах;
  - радиотехническая разведка для выявления абонентских терминалов сотовой и спутниковой связи, установления их местонахождения при выполнении поисковых работ;
  - оценка результатов применения авиационно-спасательных технологий в процессе ликвидации ЧС;

- аэрофотосъемка заданных районов с последующей топографической привязкой фотоснимков для построения ортофотопланов заданных районов, создания трехмерных моделей местности, требуемого объекта, а также видео-фото документирование объектов контроля для получения обзорных и детальных изображений;

- *специальные:*
  - обеспечение связи и ретрансляция радиосигналов;
  - оповещение населения об угрозе возникновения ЧС;
  - проведение замеров в районе химических и радиационных аварий;
- *транспортные:*
  - доставка малогабаритных грузов (индивидуальных средств спасения, мед. аптечек и др.) в назначенное место.

В МЧС России используется комплексный подход к целесообразности применения БАС для ЧС различных масштабов. Следует отметить, что использование различных беспилотных воздушных судов основано на следующих принципах применения.

- *БВС самолетного типа:*
  - оценка масштабов ЧС;
  - обследования больших районов, линейных и площадных объектов;
  - поиск требуемого объекта, оценки его общего состояния;
  - получение информации для прогнозирования дальнейшего развития ЧС.
- *БВС вертолетного типа:*
  - детальная разведка в зоне ЧС, объекта (объектов), оценки их состояния;
  - осмотр отдельных элементов строений, сооружений, в том числе и внутри них, отдельных участков местности, дорог, мостов и др.;
  - определение маршрутов движения наземных аварийно-спасательных сил и координации их действий с передачей информации в реальном масштабе времени на пункты управления.
- *БВС комбинированного типа:*
  - эффективное совмещение возможностей БВС самолетного и вертолетного типов при выполнении различных задач.

БАС широко используются для оперативной аэрофотосъемки с целью мониторинга и прогнозирования чрезвычайных ситуаций [20], в частности, создания цифровых *ортофотопланов* – цифрового трансформированного изображения местности (объекта), созданного по перекрывающимся исходным фотоснимкам. Прикладное применение цифровых ортофотопланов в МЧС России можно условно разделить на три группы, в зависимости от цели, которую планируется достигнуть:

1. Построение ортофотопланов и цифровых моделей рельефа местности с целью прогнозирования возможных последствий подтопления.

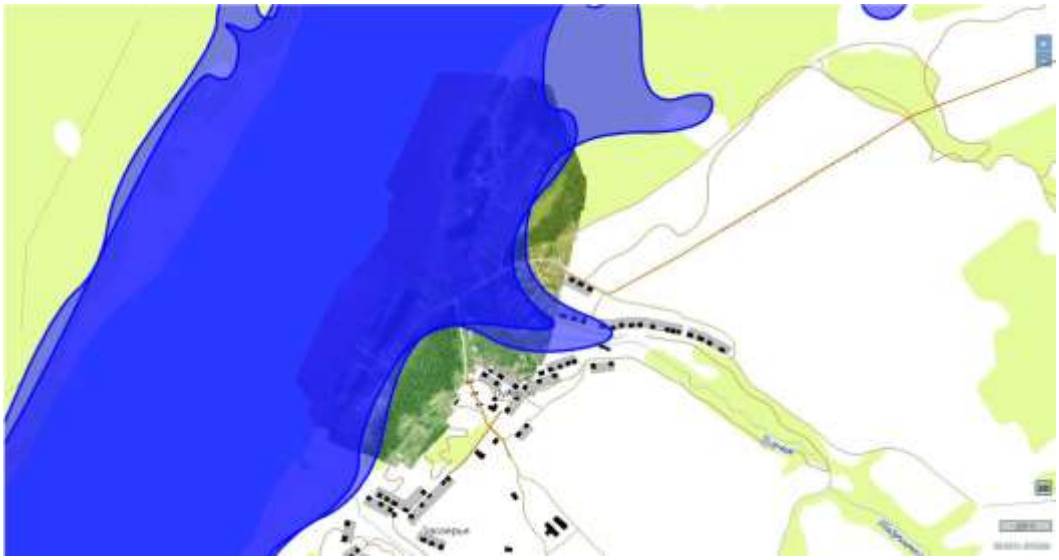

Рисунок 3.3. – Моделирование последствий подтопления.

2. Построение ортофотопланов с целью определения и тематической обработки зон подтопления и строений, попавших в эту зону.

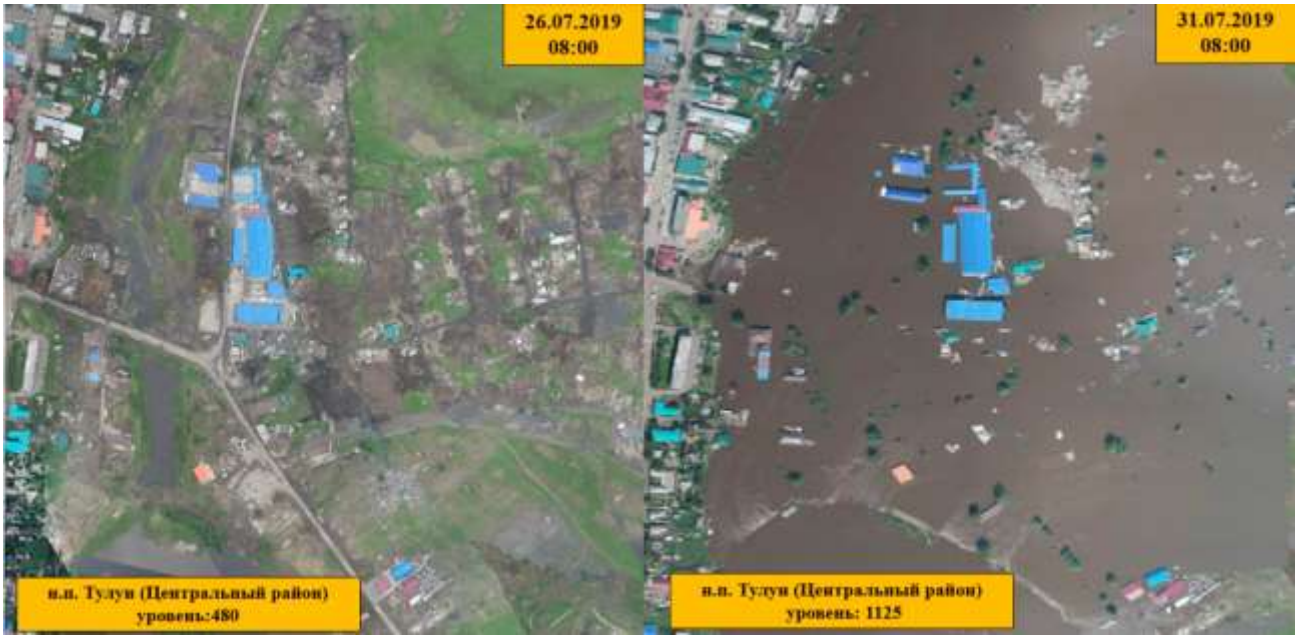

Рисунок 3.4. – Определение зон наводнения.

Рисунок 3.5. – Тематическая обработка участков, попавших в зону подтопления.

3. Анализ динамики проведения аварийно-восстановительных работ и ликвидации последствий ЧС, анализ природных явлений.

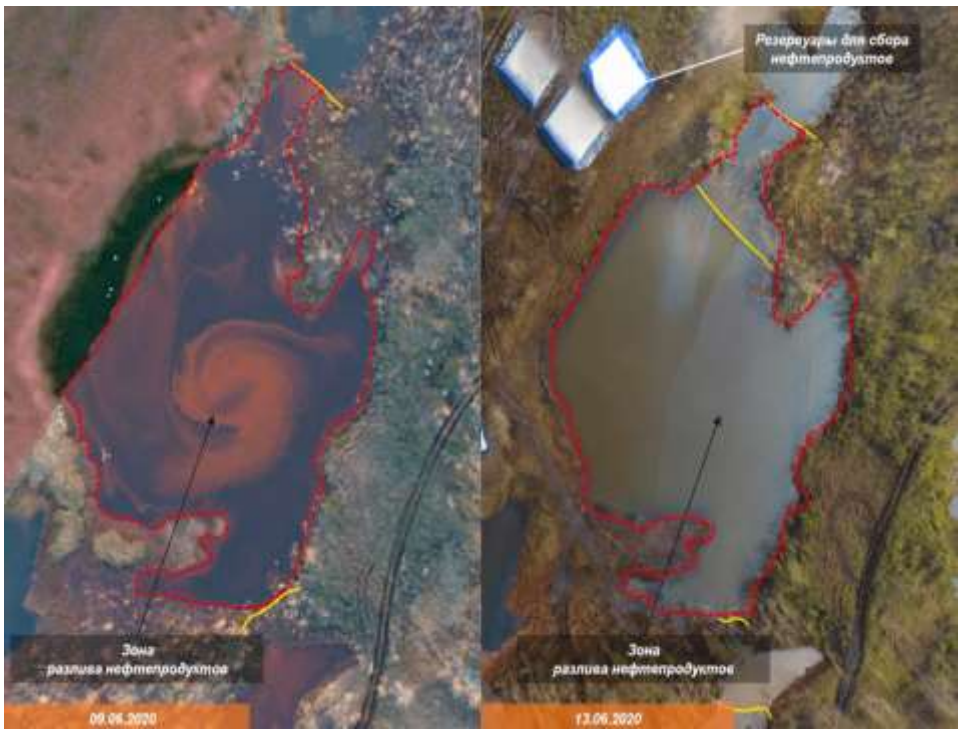

Рисунок 3.6. – Пример анализа динамики проведения работ по откачке разлившихся нефтепродуктов.

Спектр направлений применения цифровых ортофотопланов в МЧС России может быть расширен в зависимости от возникающих ЧС.

3.6 Контрольные вопросы

1. Дайте определение мониторинга.
2. Дайте определение объекта мониторинга.
3. Что входит в понятие объект мониторинга?
4. Какие уровни (ступени) мониторинга различают?
5. По каким типам могут условно подразделяться системы мониторинга?
6. Что относится опасным гидрологическим явлениям?
7. Что входит в мониторинг пожарной опасности в лесах и лесных пожаров?
8. Какие виды работ организуются при различных классах пожарной опасности?
9. Каковы основные цели применения беспилотных авиационных систем в МЧС России?

4. СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

4.1 Общие понятия СППР

Система поддержки принятия решений (СППР) или *Decision Support System (DSS)* – это компьютерная автоматизированная система, разработанная для оказания помощи людям в сложных условиях при анализе предметной деятельности с целью принятия полных и объективных решений. СППР предоставляет информацию в различных формах, таких как печатные отчеты, экранные выводы или звуковые сигналы, основываясь на входных данных, чтобы помочь людям быстро и точно оценить ситуацию и принять решение. Развитие СППР произошло благодаря объединению управленческих информационных систем и систем управления базами данных.

Для анализа и разработки предложений в системе поддержки принятия решений (СППР) применяются различные методы. Среди них можно выделить *информационный поиск*, *интеллектуальный анализ данных*, *поиск знаний в базах данных*, *рассуждение на основе прецедентов*, *имитационное моделирование*, *эволюционные вычисления* и *генетические алгоритмы*, *нейронные сети*, *ситуационный анализ, когнитивное моделирование* и другие. Некоторые из этих методов были разработаны в области искусственного интеллекта. Если СППР основывается на применении методов искусственного интеллекта, то она называется *интеллектуализированной СППР* или *ИСППР*. Основными элементами СППР являются: *база данных (база знаний)*, *модель* (контекст принятия решения и критерии пользователя) и *пользовательский интерфейс*. Близкими к СППР классами систем являются экспертные системы и автоматизированные системы управления.

Компоненты СППР могут быть классифицированы следующим образом:

- *Входы*: Факторы, числа и характеристики для анализа.
- *Знания и экспертиза пользователя*: Входы, требующие ручного анализа со стороны пользователя.
- *Выходы*: Преобразованные данные, на основе которых СППР генерирует *решения*.
- *Решения*: Результаты, генерируемые СППР на основе критериев пользователя.

Для систематизации понятий СППР можно, в частности, использовать отношение с пользователем в качестве критерия классификации. В этом случае различают пассивные, активные и совместные СППР.

- *Пассивная СППР* – это система, которая помогает процессу принятия решений, но не может предложить явные рекомендации или решения.
- *Активная СППР* способна предложить такие рекомендации или решения.
- *Совместная СППР* позволяет проводить итерационный процесс между человеком и системой с целью достижения консолидированного решения: принимающий решение (или его советник) может изменять, дополнять или уточнять рекомендации, предоставленные системой, перед отправкой их обратно в систему для проверки, и наоборот, система снова улучшает, дополняет и уточняет рекомендации принимающего решение и отправляет их обратно для проверки.

4.2 СППР в приложениях к вопросам природного и техногенного риска

За последнее десятилетие значительно возросло значение автоматизированных систем, применяемых для координации и управления деятельностью по предотвращению и ликвидации различных чрезвычайных ситуаций. Расширяется спектр функциональных задач, которые они выполняют, начиная от простого моделирования и предоставления справочной информации, и заканчивая развитием интеллектуальных систем оперативного управления и анализа данных мониторинга ситуации. В настоящее время нет устоявшегося понятия систем поддержки принятия решений (СППР) в приложениях к вопросам природного и техногенного риска. Это связано, в первую очередь, с разнообразием различных технических инструментов и классами решаемых задач. Различные подходы к СППР рассматривались в научных публикациях (см., например, [21]), учебных пособиях (см. [22]) и монографиях (см. [23], [24]).

Рассмотрим основные понятия, относящиеся к системе поддержки принятия решений в чрезвычайных ситуациях, основанные на [25, стр. 48-49].

Автоматизированная система поддержки принятия решений в чрезвычайных ситуациях (АСППР) – это система, предназначенная для информационного обеспечения процессов подготовки вариантов решений по ликвидации чрезвычайных ситуаций.

Задачи, решаемые АСППР, делятся на три основных класса:

- прогнозирование обстановки;
- оценка и контроль обстановки;
- подготовка данных для принятия решения и планирования его реализации.

Выполняя прогнозирование обстановки, АССПР выдает данные о ней на основе расчетов по специальным алгоритмам (методикам), использующим

минимум исходных данных. Контроль и оценку обстановки обеспечивают сопоставление данных, полученных из различных источников, друг с другом, а также с результатами прогнозирования, определение степени достоверности обобщенной информации с учетом ее неполноты и неопределенности, сопоставление обобщенных данных обстановки и данных о ходе проводимых мероприятий с запланированными показателями. При подготовке данных для принятия решения и планирования его реализации определяется требуемый состав, сроки проведения и объемов планируемых мероприятий, расчет рационального состава необходимых для осуществления выбранных мероприятий сил, средств и ресурсов, а также планы их применения.

Система поддержки принятия решений функционирует в режимах: *повседневной деятельности*, *повышенной готовности* и *чрезвычайной ситуации*. Разделение функций между режимами делается по принципу – все трудоемкие и длительные операции, связанные с информационным наполнением системы данными и знаниями, выполняются в повседневном режиме. В оперативном режиме выполняются только «быстрые», вычислительно эффективные операции, в первую очередь по использованию накопленных в системе данных и знаний в конкретной ситуации. Таким образом, АСППР функционирует в рамках следующих основных процессов:

- заблаговременное прогнозирование и оценка развития возможных чрезвычайных ситуаций, как без учета, так и с учетом проведения соответствующих мероприятий по предупреждению, локализации и ликвидации чрезвычайных ситуаций;
- создание и ведение базы оперативных ситуационных планов действий в возможных чрезвычайных ситуациях;
- моделирование хода и результатов мероприятий с целью оценки эффективности планов;
- оперативный прогноз и оценка сложившейся обстановки при возникновении чрезвычайных ситуаций;
- разработка варианта плана мероприятий с использованием базы ситуационных планов.

В результате формируется конкретный ситуационный план ликвидации чрезвычайных ситуаций, обладающий высокой степенью практической применимости, устойчивости к возможным отклонениям и обоснованности, принятых в нем решений. Информационная структура такого плана включает:

- план по составу, объемам и срокам проведения аварийно-спасательных работ;
- план привлечения сил и средств для ликвидации чрезвычайных ситуаций;
- план обеспечения продовольственными, медицинскими, материально-техническими и др. ресурсами;
- план перевозок сил, средств и ресурсов, привлекаемых для ликвидации чрезвычайных ситуаций.

Для эффективного управления безопасностью территорий необходимо единое информационное пространство, охватывающее все уровни управления от объектового до федерального. Современные информационные технологии предлагают разнообразные инструменты для построения интегрированных систем поддержки оперативного управления. Система поддержки принятия решений включает следующие компоненты:

1. *Базы данных и системы сбора данных* предназначены для актуализации информации об источниках риска, инфраструктуре территорий, состоянии сил и средств, а также для описания их использования и взаимодействия. В качестве перспективной технологии для сбора и обновления данных используется web-технология.

2. *Средства анализа данных* необходимы для обработки данных мониторинга обстановки, формирования агрегированных показателей и планирования превентивных мероприятий по снижению рисков чрезвычайных ситуаций.

3. *Геоинформационный модуль* предназначен для оперативного отображения обстановки, пространственного анализа данных, моделирования процессов управления и визуализации динамики чрезвычайных ситуаций.

4. *Модуль формирования решений*, который будет использоваться для оперативного создания донесений, отчетов и справочной информации. Кроме того, пользователю предоставляются средства быстрого доступа к слабо формализованным документам.

СППР могут применяться в самом широком смысле для различных режимов: при наводнениях, стихийных бедствиях, пожарах, пандемии, и т.д. Приведем некоторые примеры международных СППР.

Примером глобальной СППР является международный *Портал управления рисками и устойчивостью* (Инициатива Азиатско-Тихоокеанской сети по обеспечению устойчивости к стихийным бедствиям

https://rrp.unescap.org/decision-support-system,

который обеспечивает контекстуальный анализ различных опасностей, рисков и уязвимости, социально-экономическую информацию для поддержки принятия обоснованных решений. Используя различные инструменты, пользователи могут легко понять расположение зон риска, что делает их рискованными и, наконец, определить средства для снижения этих рисков и адаптации к ним.

Другой пример – концепция интеллектуальной системы поддержки принятия решений при стихийных бедствиях (IDDSS) для городских катастроф

https://www.unimelb.edu.au/cdmps/research/research-projects/iddss,

которая объединяет интеллектуальную геопространственную платформу с усовершенствованным механизмом моделирования оптимизации, разработанная в университете Мельбурна.

Национальная система управления инцидентами (NIMS) США

https://www.fema.gov/emergency-managers/nims

помогает всем уровням правительства, неправительственным организациям и частному сектору работать вместе над предотвращением, защитой, смягчением последствий инцидентов, реагированием на них и восстановлением после них.

В качестве российских разработок приведем пример системы интеллектуальной поддержки принятия решений по ликвидации ЧС ЭСПЛА-ПРО [26]. Экспертная геоинформационная система ЭСПЛА-ПРО разработана в 2004-2007 годах по заказу Агентства по делам ГО и ЧС Красноярского края для поддержки деятельности оперативной дежурных смен ЦУКС.

Технологии, реализованные в системе ЭСПЛА-ПРО, позволяют решать важнейшие задачи органов управления МЧС:

1. Обеспечение оперативного управления в кризисных ситуациях в повседневном режиме функционирования: мониторинг и контроль обстановки, работа с прогностической и аналитической информацией.
2. Обеспечение оперативного управления в режиме повышенной готовности и в режиме ЧС: моделирование масштабов и последствий стихийных бедствий, техногенных аварий и катастроф, формирование оперативных отчетных форм и рекомендаций по действиям в ЧС.

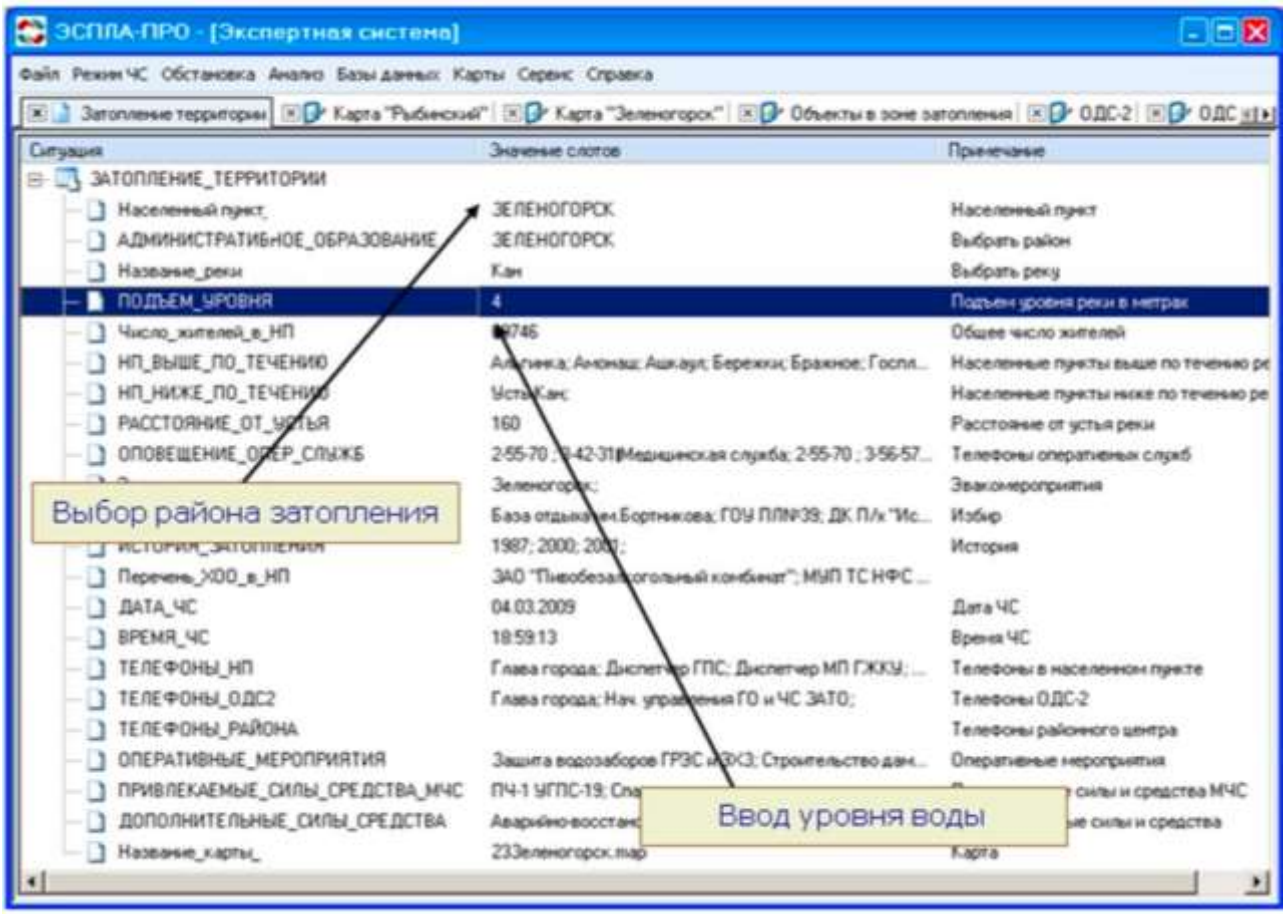

Рисунок 4.1. – Экспертная геоинформационная система ЭСПЛА-ПРО.

Решение этих задач выполнено на основе интеграции современных информационных технологий: экспертных и геоинформационных систем, систем управления базами данных, OLAP-анализа и других. За счет интеграции технологически разнородных элементов реализованы принципиально новые информационные модели. Основные компоненты системы – геоинформационная система, блок расчетных методик, система оперативного анализа данных могут использоваться и как самостоятельные программы. В режиме ЧС работой компонентов управляет экспертная система, вызывающая по мере необходимости ГИС, математические модели оценки обстановки, модель формирования отчетных форм и другие. Базы данных, знаний и картографические базы составляют информационные ресурсы системы.

В системе ЭСПЛА-ПРО реализованы сценарии аварийных ситуаций, характерных для промышленных объектов. Реализованы модули оценки последствий химических аварий, пожаров нефтепродуктов, взрывов твердых веществ, пыли и топливовоздушных смесей. В качестве выходных данных

система оперативно формирует документы, позволяющие организовать экстренное реагирование до сбора комиссий по ЧС и ПБ.

Другой пример – распределенная геоинформационная система «Шахты» [27]. Программный комплекс работает в двух режимах: *повседневном*, когда осуществляется сбор и анализ данных, и *оперативном* (*режим ЧС*).

В повседневном режиме происходит сбор и актуализация данных согласно регламенту обновления базы данных. Пополнение и корректировка информационных таблиц (семантики), содержащих характеристики потенциально опасных объектов, данные о территориях, инфраструктуре, силах и средствах происходит 2-3 раза в год. Мониторинг (суточные донесения) состояния аварийно-спасательных и других формирований заполняется ежедневно.

В режиме ЧС система выполняет следующие функции: визуализация порядка прикрытия и реагирования сил и средств подразделений МЧС России и других взаимодействующих структур на ЧС (происшествия) на шахтах с визуализацией состава и местоположения первого эшелона группировки, схем проезда до места ЧС с оценкой времени в пути, формирование первичного документооборота в соответствии с табелем срочных донесений МЧС РФ.

Одно из важных преимуществ системы – интерактивная детализация данных. Лицо, принимающее решения, может использовать данные в большем объеме по сравнению с требованиями форм табеля срочных донесений МЧС России. Модуль формирования решений позволяет уточнять данные, делая интерактивные запросы к базам данных их геоинформационного модуля и электронных форм донесений. Это существенно повышает оперативность работы по сравнению с банком паспортов объектов и территорий.

4.3 Ситуационные центры

Ситуационные центры создаются для оперативного управления и предназначены для управления крупными государственными структурами, такими как МЧС, ГИБДД, МВД и другие организации федерального или муниципального уровня. Ситуационный центр – это инструмент для решения различных задач, в частности:

- мониторинг обстановки и состояния объекта управления с прогнозированием развития ситуации на основе анализа поступающей информации, а также предоставления руководству обработанной и классифицированной информации определенного формата;

- повышение эффективности при коллективной работе группой экспертов и аналитиков, оптимизация принятия решений;
- моделирование развития ситуаций, последствий управленческих решений на базе использования информационно-аналитических систем;
- комплексное информационное обеспечение руководства;
- контроль процессов в кризисных ситуациях, оперативная обратная связь при выходе ключевых показателей за границы нормы.

Главные требования к ситуационным центрам включают:

- быстрый отклик на текущие события;
- сбор и обработка обширного объема информации из различных источников данных одновременно;
- непрерывная работа в режиме 24/7.

В структуру типового ситуационного центра могут входить:

- *Центр мониторинга*, основные задачи которого: сбор и обработка информации, определение нештатных событий по заданным критериям, оперативное реагирование на события, передача информации в аналитический отдел, подготовка для аналитиков и экспертов информации в классифицированном и систематизированном виде; основные пользователи – это операторы, которые работают в течение длительного времени.
- *Аналитический центр*, в котором работают группы аналитиков, результатом их работы отчет, прогноз развития, оперирующий определенной моделью, которая поступает в центр принятия решений с указанием приоритета задач и степени критичности ситуации.
- *Центр принятия решений*, который является стратегическим пространством для совещания руководства. Как правило, в принятии решений участвуют ограниченное число лиц, поэтому им требуется возможность максимально сосредоточиться на предоставленной экспертами информации.

Ситуационные центры сегодня используются:

- федеральными органами государственной власти;
- региональными органами субъектов РФ и местного самоуправления (краевые и областные администрации, мэрии и др.);
- крупными промышленными предприятиями в отраслях энергетики, нефтегазовой, транспортной и др;

- образовательными учебными учреждениями и др.

4.3.1 Примеры известных российских ситуационных центров

Ситуационный центр Московского метрополитена. Ситуационный центр предназначен для обработки в режиме реального времени всех сигналов о чрезвычайных ситуациях, происходящих на территории метрополитена. Созданный программно-аппаратный комплекс позволяет операторам ситуационного центра устанавливать двустороннюю аудио-связь со станциями метрополитена, контролировать обстановку с помощью системы видеонаблюдения, организовывать видеоконференцсвязь со службами метрополитена и других ведомств.

Ситуационный центр Рособрнадзора. Ситуационный центр предназначен для разработки, оперативного анализа и реализации мер, направленных на повышение объективности единого государственного экзамена и проведение его без нарушений.

Ситуационный центр ЦОДД Москвы. Ситуационный центр предназначен для регулирования работы интеллектуальной транспортной системы г. Москвы. Основное направление развития – интеграция всей системы, построение системы управления дорожным движением, работа светофорных объектов, дорожных знаков, информационных табло.

Ситуационный центр Российской академии государственной службы при Президенте РФ. Центр предназначен для поддержки ресурсами и средствами разнообразных активных форм проведения занятий со слушателями всех видов и форм обучения; поддержки ресурсами и средствами научно-исследовательских и информационно-аналитических работ, проводимых в академии, обучения персонала ситуационных центров использованию современных информационных, аналитических и технологических средств; проведения деловых игр по заявкам органов государственной власти и местного самоуправления; стендовой отработки интеллектуальных информационных технологий и создание прототипов рабочих технологий федеральных органов власти.

Центр управления в кризисных ситуациях МЧС России (ЦУКС) – головной орган управления РСЧС, осуществляющий повседневное управление силами и средствами РСЧС при проведении аварийно-спасательных и других неотложных работ при ликвидации чрезвычайных ситуаций на территории

России. Осуществляет согласованную деятельность со структурными подразделениями центрального аппарата министерства, с региональными центрами ГОЧС, органами, специально уполномоченными решать задачи гражданской обороны, задачи по предупреждению и ликвидации чрезвычайных ситуаций при органах исполнительной власти субъектов РФ и органах местного самоуправления, с органами управления систем мониторинга, прогнозирования чрезвычайных ситуаций, аварийно-спасательными формированиями федеральных органов исполнительной власти, а также с соответствующими органами управления зарубежных стран. На Центр возложены функции обеспечения оперативной готовности дежурных смен подведомственных МЧС России пунктов управления к выполнению поставленных задач. После выдачи сигналов о переводе РСЧС в режим военного времени функции головного пункта управления РСЧС осуществляет центральный командный пункт МЧС России.

Основными задачами Центра являются:

- оперативное реагирование на угрозу возникновения чрезвычайных ситуаций;
- поддержание устойчивого оперативного управления дежурными силами и средствами в системе МЧС России;
- участие в управлении мероприятиями гражданской обороны при угрозе или возникновении военных действий; координация деятельности органов повседневного управления РСЧС при ликвидации чрезвычайных ситуаций;
- сбор и обработка оперативной информации в ходе проведения аварийно-спасательных работ при ликвидации чрезвычайных ситуаций;
- участие в мероприятиях по созданию, развитию и обеспечению устойчивого функционирования АИУС РСЧС.

Состоит из управлений: *оперативного реагирования*, *оперативно-аналитического*, *информационно-технического*, а также *подразделений обеспечения*.

4.4 Контрольные вопросы

1. Опишите компоненты общей системы поддержки принятия решений
2. Какие задачи решает Автоматизированная система поддержки принятия решений в чрезвычайных ситуациях (АСППР), предназначенная для информационного обеспечения процессов подготовки вариантов решений по ликвидации чрезвычайных ситуаций?

3. Какие компоненты включает в себя система поддержки принятия решений?
4. Приведите примеры зарубежных СППР в приложениях к вопросам природного и техногенного риска.
5. Приведите примеры российских СППР в приложениях к вопросам природного и техногенного риска.
6. С какой целью создаются ситуационные центры?
7. Опишите структуру и требования к ситуационным центрам.
8. Приведите примеры известных российских ситуационных центров.

5. ГЕОГРАФИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Географическая информационная система (ГИС) – это система, которая создает, управляет, анализирует и отображает все типы географических данных. ГИС соединяет данные с картой, интегрируя данные о местоположении со всеми типами описательной информации. Это обеспечивает основу для картографирования и анализа, которые используются в науке и практически в каждой отрасли промышленности. ГИС помогает пользователям понимать закономерности, взаимосвязи и географический контекст. Преимущества включают улучшенную коммуникацию и эффективность, а также более эффективное управление и принятие решений. Технологии ГИС применяют географическую науку с помощью инструментов для понимания и совместной работы.

Федеральный закон о геодезии и картографии [28] устанавливает правила для деятельности, связанной с созданием, поиском, хранением, обработкой, предоставлением, использованием и распространением пространственных данных, в том числе с применением геоинформационных технологий, систем и средств.

Согласно ГОСТ Р 52438-2005 2018 [29], *геоинформационная система* (ГИС), – это информационная система, оперирующая пространственными данными.

По пространственному охвату различают *глобальные*, *субконтинентальные*, *национальные*, *межнациональные*, *региональные*, *субрегиональные* и *локальные* ГИС. В Российской Федерации принято различать *федеральные* ГИС (ФГИС), *региональные* (РГИС), *муниципальные* (МГИС) и *локальные* (ЛГИС).

По различным платформам разработки ГИС можно разделить на *настольные ГИС* (устанавливаемые на десктопах), *веб-ГИС* (системы, доступные в веб-браузерах, позволяющие просматривать, редактировать и проводить анализ пространственных данных в сети Интернет/Интранет) и *мобильные ГИС* (доступные в мобильных устройствах). Кроме того, можно выделить *корпоративные ГИС* – это многопользовательские геоинформационные системы, предназначенная для автоматизации бизнес-процессов организации.

К основным рассматриваемым нами понятиям относятся *геопорталы* – системы поиска пространственных данных по их описанию (метаданным), *база пространственных данных* (совокупность пространственных данных, организованных по определенным правилам, устанавливающим общие

принципы описания, хранения и манипулирования данными, предназначенная для удовлетворения информационных потребностей пользователя), а также *ГИС-сервисы* – веб-сервисы, обеспечивающие доступ к пространственным данным, облегчающие их обработку, анализ, поиск и визуализацию.

Также, к основным понятиям относится *фотограмметрическая обработка снимков*, которая позволяет проводить геокодирование, ортотрансформирование, создание цифровых моделей рельефа (ЦМР) и местности (ЦММ). Фотограмметрия включает в себя:

- создание *ортофотопланов* (фотографического плана местности на точной геодезической основе, полученного путем аэрофотосъемки или космической съемки с последующим преобразованием снимков из центральной проекции в ортогональную с помощью метода ортотрансформирования);
- создание бесшовных *ортофотомозаик* (ортомозаика – результат яркостного выравнивания и объединения («сшивки») нескольких ортотрансформированных изображений (снимков) в одно непрерывное изображение с заранее заданным изобразительным качеством);
- создание *цифровых моделей рельефа и местности* (ЦМР).

Отметим, что указать все доступные Интернет-ресурсы и ГИС-системы невозможно, более того, данные ссылки актуальны только на момент написания данного пособия.

5.1 Обзор основных ГИС

Сделаем краткий обзор некоторых основных ГИС широкого применения.

5.1.1 ArcGIS

ArcGIS – это коммерческая комплексная система, которая предоставляет возможности по сбору, организации, управлению, анализу, обмену и распределению географической информации. Она является лидером среди мировых платформ для создания и использования геоинформационных систем (ГИС) и используется людьми по всему миру в области государственного управления, бизнеса, науки, образования и СМИ для применения географических знаний на практике. Платформа ArcGIS позволяет опубликовать географическую информацию для доступа и использования ею любыми пользователями в любой точке мира, где возможно использование веб-браузеров, мобильных устройств,

таких как смартфоны, и настольных компьютеров. Например, с использованием платформы ArcGIS компания ESRI (США) разработала карты рисков затопления Восточного побережья США на основе моделирования штормовых нагонов, вызванных ураганами.

- **ArcGIS Online** – облачное программное обеспечение для создания интерактивных веб-карт и обмена ими [30].
- **ArcGIS Pro** – это профессиональное настольное ГИС-приложение, которое позволяет создавать расширенные 2D- и 3D-карты, визуализации и анализ данных. В дополнение к ArcGIS Pro, лицензия пользовательского типа GIS Professional включает полный доступ к ArcGIS Online [31, 32].

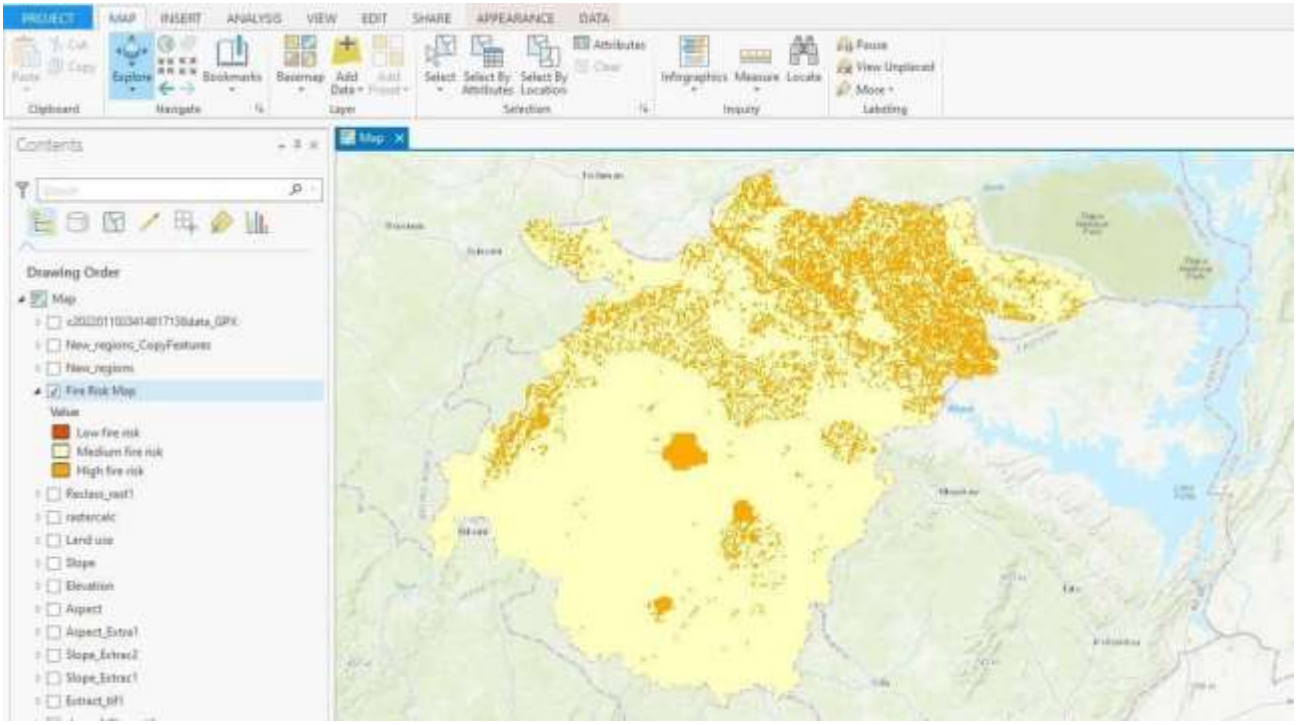

Рисунок 5.1. – Пример использования ArcGIS: карта пожарной опасности Восточного региона Ганы

5.1.2 QGIS

QGIS Desktop – это настольная ГИС с открытым кодом, которая работает на **Linux**, **macOS**, **Windows** и **Android**, обладающая широкими возможностями. Огромную популярность **QGIS** приобрело благодаря своей бесплатности, широкой поддержке сообщества и расширяемости на основе различных плагинов. К достоинствам системы можно отметить: возможности просмотра данных, исследование данных и создание масштабируемых карт с использованием различных слоев, управление данными: создание,

редактирование и экспорт, анализ данных и возможность публикации карт в сети Интернет [33, 34].

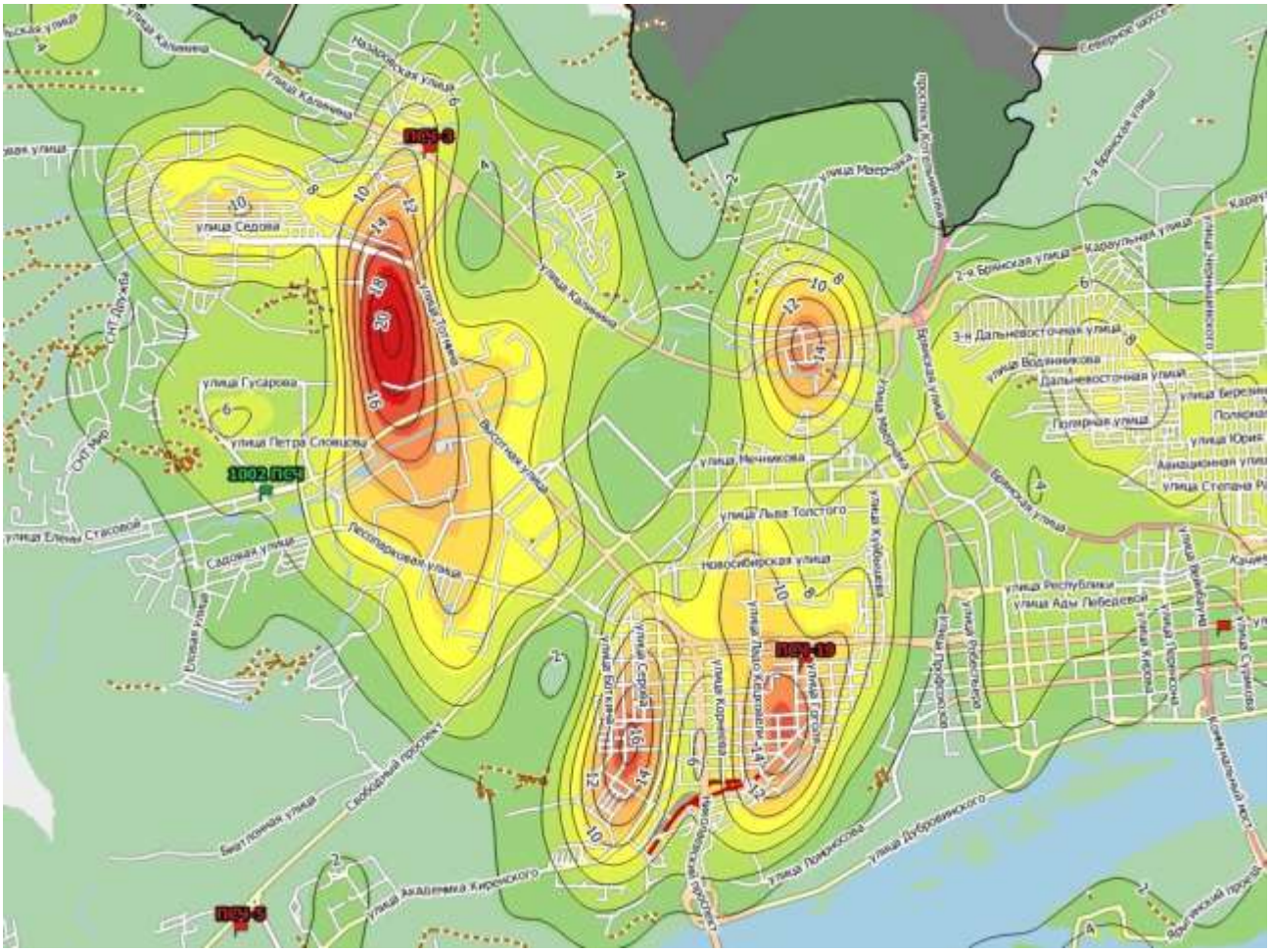

Рисунок 5.2. – Пример карты плотностей пожаров в QGIS.

5.1.3 NextGIS

NextGIS – это семейство ГИС-программ российских разработчиков, включенное в Единый реестр российских программ [35].

Далее сделаем некоторый обзор федеральных, ведомственных и международных геопорталов, которые могут представлять интерес в деятельности МЧС России, включающее в себя

- **NextGIS Web** – серверная веб-ГИС для хранения данных в облаке с возможностью отображения их как геопорталы;
- **NextGIS QGIS** – полнофункциональную настольную ГИС для создания и редактирования данных, производства карт, выполнения аналитических операций;
- **NextGIS Mobile** – для работы на носимых устройствах;

- **NextGIS Data** – каталог ГИС-данных различного уровня.

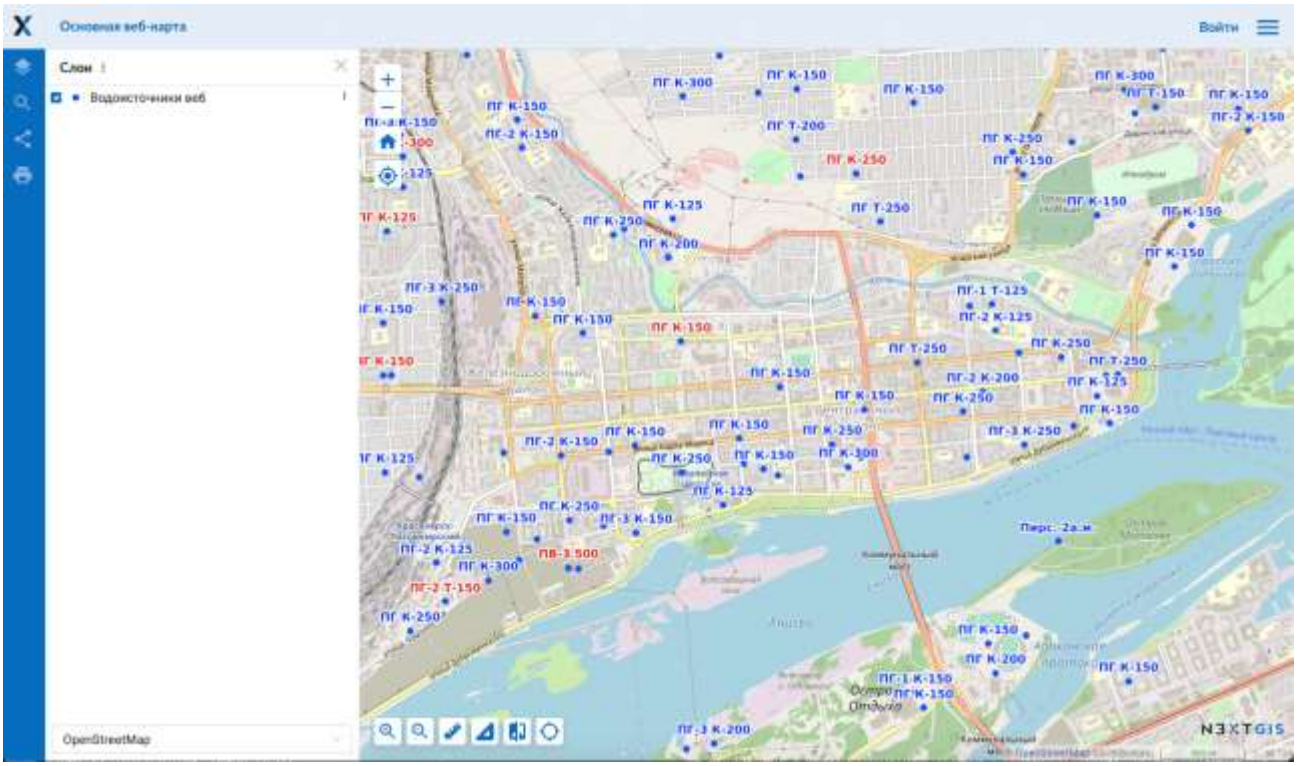

Рисунок 5.3. – Пример использования NextGIS для отображения карты водоисточников.

5.2 Федеральные геопорталы

Охарактеризуем некоторые основные геопорталы пространственных данных, доступные в России.

5.2.1 Федеральный портал пространственных данных

На данном портале [36] можно получить следующую информацию:

- Сведения Единой электронной картографической основы (ЕЭКО);
- Картографические материалы, ортофотопланы, материалы дистанционного зондирования Земли;
- Сведения о пунктах государственных геодезической, нивелирной, гравиметрической сетей, геодезических сетей специального назначения.

В частности, посредством федерального портала все заинтересованные физические и юридические лица могут получать пространственные данные федерального фонда пространственных данных (ФФПД) и сведения единой электронной картографической основы (ЕЭКО).

На федеральном портале пространственных данных для федеральных органов исполнительной власти, органов власти субъектов и органов местного самоуправления доступны следующие услуги:

- предоставление пространственных данных и материалов федерального фонда пространственных данных;
- предоставление сведений единой электронной картографической основы.

5.2.2 Федеральная ГИС территориального планирования (ФГИС ТП)

Данная информационно-аналитическая система [37] обеспечивает доступ к сведениям, содержащимся в государственных информационных ресурсах, государственных и муниципальных информационных системах, в том числе в информационных системах обеспечения градостроительной деятельности, и необходимым для обеспечения деятельности органов государственной власти и органов местного самоуправления в области территориального планирования. Система содержит цифровые топографические карты и планы открытого пользования.

5.2.3 Геопортал Роскосмоса

Геопортал Роскосмоса – геоинформационный ресурс [38] для доступа к единому банку данных дистанционного зондирования (ДЗЗ) Земли из космоса. Геопортал Роскосмоса – ресурс, который сочетает в себе средство просмотра космических снимков земной поверхности и средство поиска данных ДЗЗ с российских спутников по наиболее полному в России каталогу. Отличительной особенностью Геопортала Роскосмоса является оперативная публикация данных (для просмотра в полном пространственном разрешении), поступающих с космических аппаратов.

5.3 Геопорталы в области пожарной и техносферной безопасности в Российской Федерации

Основные геопорталы, которые мы рассмотрим тут, предназначены для отображения данных дистанционного зондирования Земли для регистрирования термических точек. В качестве их пользователей могут быть Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, юридические и физические лица, использующие данные дистанционного зондирования Земли в своих интересах.

5.3.1 Информационная система дистанционного мониторинга Федерального агентства лесного хозяйства (ИСДМ-Рослесхоз)

Информационная система «ИСДМ-Рослесхоз» представляет собой распределенную сеть, состоящую из нескольких блоков и подсистем, физически расположенных в центральном узле в Пушкино и региональных узла. Особенностью системы является комплексный анализ данных о лесных пожарах из разных источников, таких как метеоданные, результаты наземного и авиамониторинга региональных лесопожарных служб, и данные космического мониторинга. При этом основой системы служат данные дистанционного зондирования Земли, позволяющие формировать объективную информацию о пожарах. Уникальной особенностью системы является наличие обратной связи – поступление данных о подтверждении или опровержении загораний, зафиксированных из космоса [39]. Система была введена в эксплуатацию в 2005 году. Сейчас, в процессе обслуживания информационной системы, проводятся ежегодные работы по обновлению границ зон мониторинга, лесного фонда, авиаотделений и лесничеств перед наступлением пожароопасного сезона. Эти работы основаны на использовании цифровых картографических материалов, предоставленных субъектами Российской Федерации. Для выполнения этой задачи была разработана геоинформационная технология, которая в дальнейшем была усовершенствована с учетом требований к картографической информации.

Спутниковый мониторинг в ИСДМ Минприроды России позволяет решать целый спектр задач. Это включает получение информации для оценки синоптической обстановки, обнаружение потенциальных зон лесных пожаров на охраняемых территориях, обнаружение и контроль динамики пожаров на неохраняемых территориях, а также оценку площадей, затронутых лесными пожарами.

К основным задачам ИСДМ-Рослесхоз можно отнести:

1. Мониторинг пожарной опасности в лесах и лесных пожаров:
   - обеспечение регионов сведениями о пожарной опасности в лесах;
   - обнаружение лесных пожаров (особенно в зоне контроля);
   - мониторинг и прогнозирование распространения крупных лесных пожаров;
   - обеспечение лесопожарных служб комплексной информацией дистанционного мониторинга и инструментами для ее анализа.
2. Контроль организации охраны лесов в регионах:

– оценка достоверности сведений о пожарной опасности в лесах;
– контроль профилактических выжиганий;
– информационное обеспечение контрольно-надзорных мероприятий.

3. Формирование однородной и объективной информации о лесных пожарах и их последствиях для:
   – подготовки сведений о лесных пожарах для Единой межведомственной информационно-статистической системы (ЕМИСС);
   – подготовки сведения о лесных пожарах для включения формы 7-ОИП (отчетность регионов об исполнении лесных полномочий в части возникших лесных пожаров);
   – проверки информации, поступающей в государственный лесной реестр.

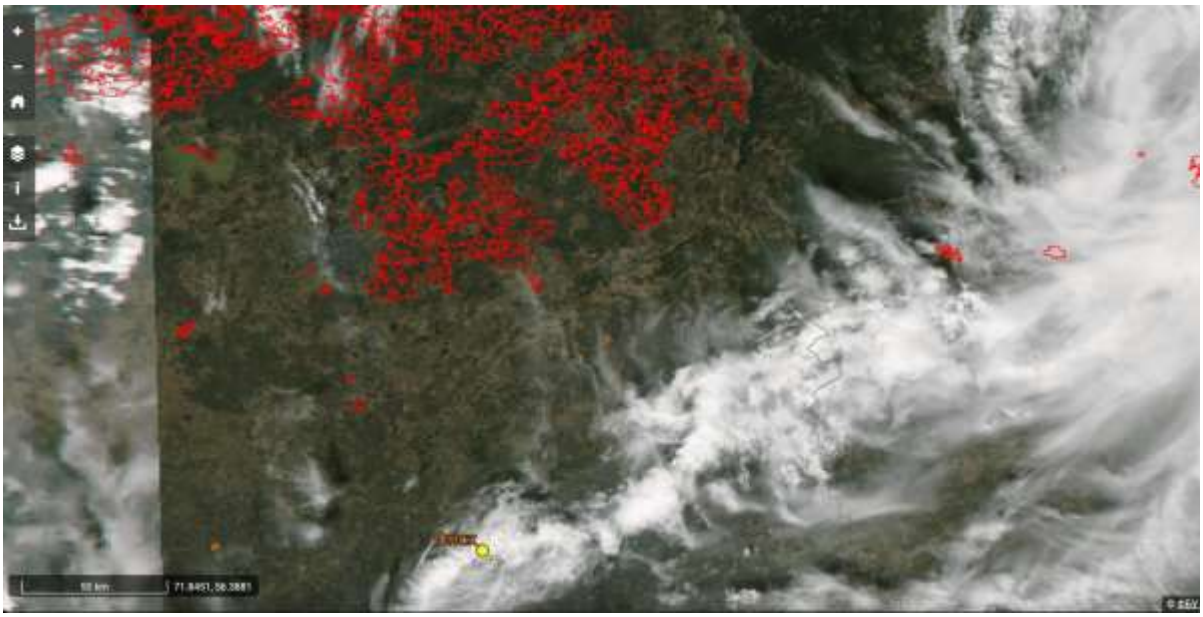

Рисунок 5.4. – Открытые данные ИСДМ-Рослесхоз.
(Информационная система дистанционного мониторинга
Федерального агентства лесного хозяйства)

5.3.2 Карта пожарной обстановки на особо охраняемых природных территориях федерального значения (ООПТ)

Портал [40] (заказчик ФГБУ «РФИ Минприроды России») содержит термоточки на ООПТ, динамику изменения пожарной обстановки, непосредственно пожарную обстановку на карте и дополнительную информацию: оперативную информацию Рослесхоза и метеорологический показатель пожароопасности.

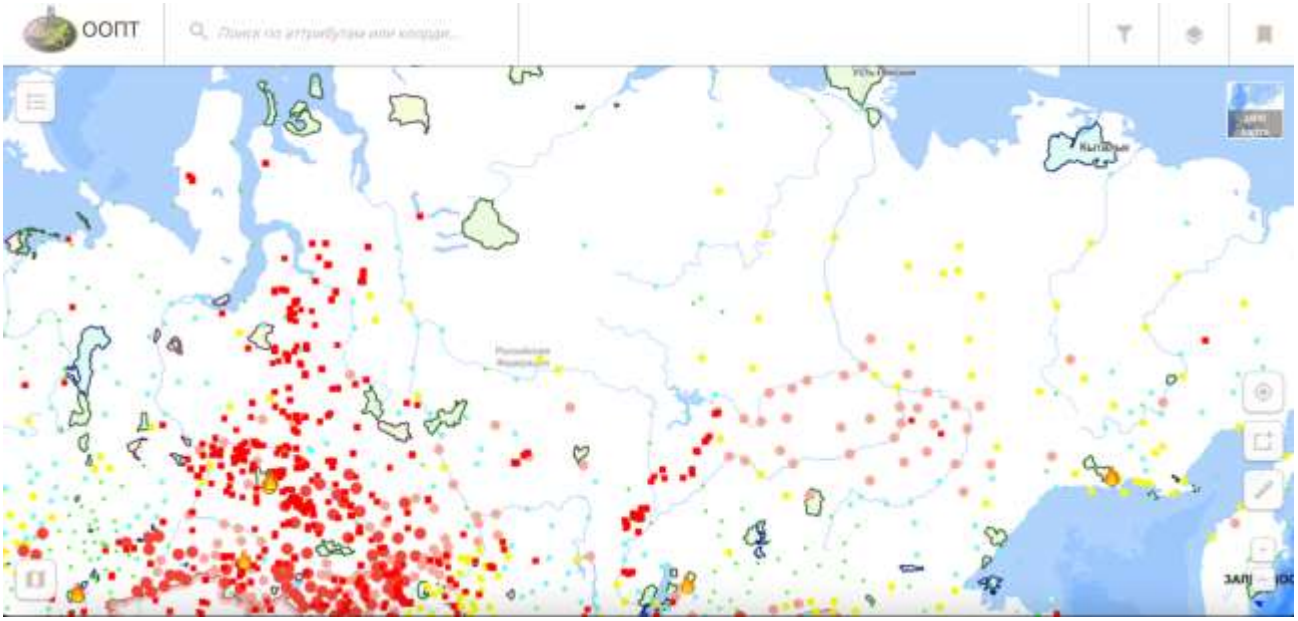

Рисунок 5.5. – Карта пожарной обстановки на особо охраняемых природных территориях федерального значения.

5.3.3 Геоинформационная система МЧС России «Космоплан»

Специалистами «СКАНЭКС» была создана ГИС «Космоплан» с доступом через локальную сеть МЧС для специалистов Управления космического мониторинга НЦУКС МЧС и офицеров дежурных смен в НЦУКС и региональных ЦУКС [41]. Созданная информационная система позволила:

- увеличить оперативность и полноту получения информации для предоставления отчетных документов со стороны специалистов Управления по космическому мониторингу о наличии требуемых космических данных по определенной территории;
- интегрировать данные системы космического мониторинга МЧС;
- повысить качество производных продуктов космосъемки за счет автоматизации обработки и наличия инструментов работы с данными;
- создать каталог ситуационных карт и отработать методику анализа обстановки в зоне ЧС;
- усовершенствовать систему формирования отчетных документов по данным космического мониторинга;
- создать технологию 3D-визуализации для оценки ситуации в зоне ЧС с использованием высокоточной информации о рельефе местности и оперативной космической съемки.

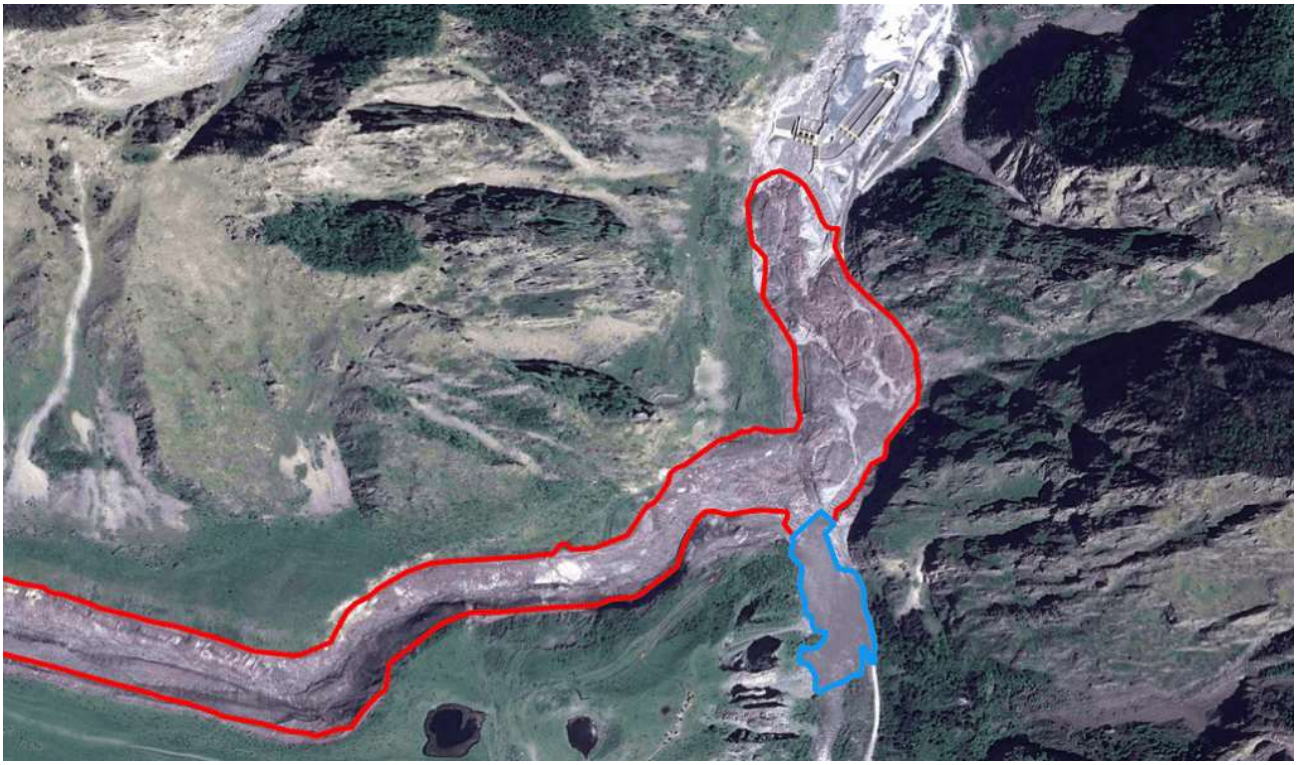

Рисунок 5.6. – Карта: место схода селя, перегородившего реку Терек. По снимку отмечено тело селя и образовавшееся подпорное озеро.

5.4 Примеры региональных порталов пространственных данных

КГАУ «Лесопожарный центр» создано для тушения лесных пожаров и осуществления противопожарных мероприятий в лесах Красноярского края. Центр выполняет функции специализированного учреждения по обеспечению полномочий в сфере лесного хозяйства, переданных органам государственной власти Красноярского края федеральным центром и предоставляет карту лесных пожаров на территории Красноярского края [42].

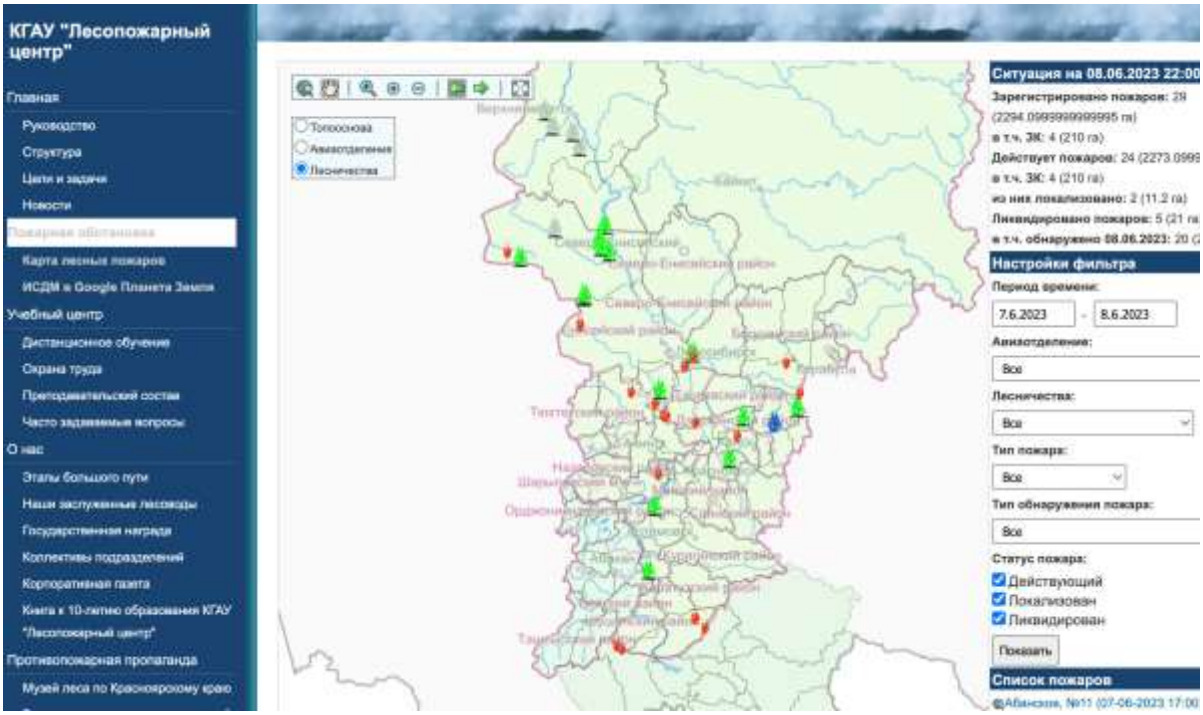

Рисунок 5.7. – Карта лесных пожаров на территории Красноярского края от КГАУ «Лесопожарный центр».

5.5 Некоторые зарубежные геопорталы

5.5.1 NASA FIRMS (Fire Information for Resource Management System)

Данный портал предоставляет данные об активных термических точках для мониторинга и последующих приложений почти в реальном времени. Система управления информацией о пожаре для ресурсов (FIRMS) распространяет данные об активном пожаре в режиме, близком к реальному времени, полученные с помощью спектрорадиометра изображений среднего разрешения (MODIS) на спутниках Aqua и Terra и набора радиометров изображений в видимом инфракрасном диапазоне (VIIRS) на спутниках S-NPP и NOAA 20 (официально известного как JPSS-1). Во всем мире эти данные доступны в течение 3 часов спутникового наблюдения, но в США и Канаде активные данные о пожарах доступны в режиме реального времени [43].

5.5.2 Global Forest Watch

Портал *Global Forest Watch* предоставляет информацию и мониторинг глобального состояния лесов, в частности, в области лесных пожаров [44].

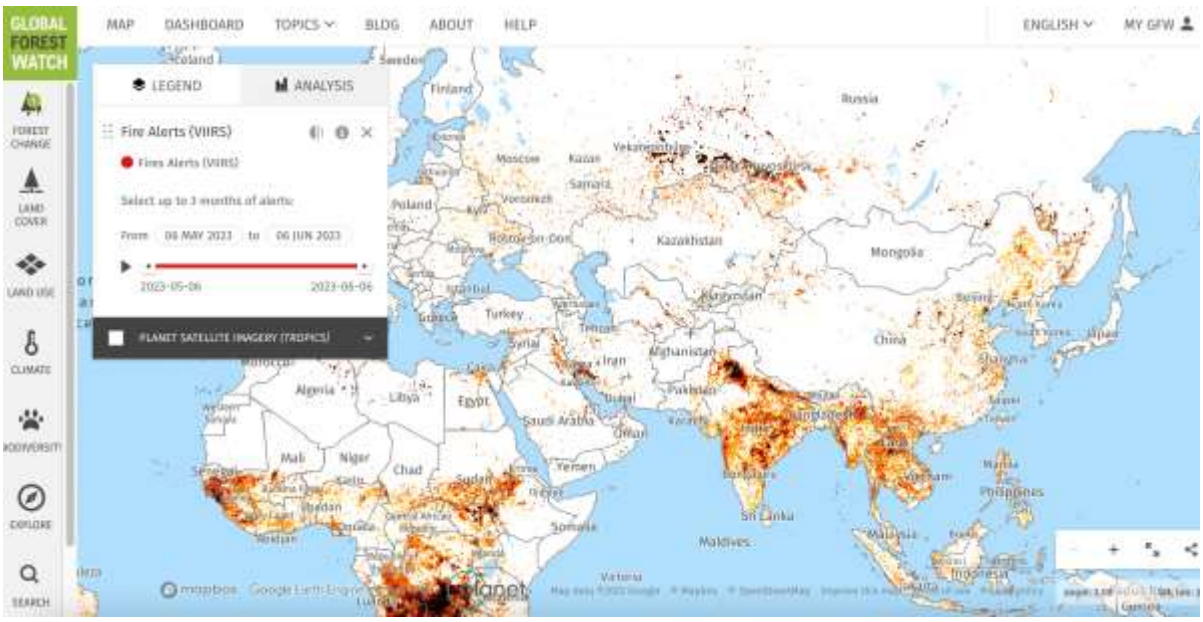

Рисунок 5.8. – Портал глобального лесного мониторинга Global Forest Watch.

Также, можно отметить некоторые другие порталы, например, [45].

5.6 Контрольные вопросы

1. Дайте определение ГИС.
2. Как ГИС различают по пространственному охвату?
3. Как можно разделить ГИС по платформам разработки?
4. Что такое геопортал?
5. Дайте определение ортофотоплана.
6. Перечислите основные известные настольные ГИС.
7. Перечислите известные вам геопорталы в области пожарной и техногенной безопасности в Российской Федерации.
8. Перечислите известные вам зарубежные геопорталы в области пожарной и техногенной безопасности.

6. КОМПЬЮТЕРНЫЕ СЕТИ

Компьютерные сети являются в настоящее время основным инструментом для обмена информацией между компьютерами пользователей (альтернативой является перенос информации на USB-носителях, твердых дисках, иногда даже дискетах). Использование компьютерных сетей дает как значительные преимущества, так и недостатки. К преимуществам относятся:

1. Возможность совместного использования вычислительных и других ресурсов в сети, таких как устройства хранения.
2. Возможность оперативного автоматизированного обмена информацией между компьютерами, обычно с использованием заранее заданных API (*Application Programming Interface* – программный интерфейс приложения), формализованных протоколов программного взаимодействия.
3. Возможность централизованного хранения информации, с контролем целостности и актуальности из единого места (единая база данных, единый реестр объектов и т.д.).

Недостатки компьютерных сетей являются обратной стороной их достоинств:

1. Проникновение в компьютерную сеть возможно из любого узла сети (рабочей станции, роутера, маршрутизатора, устройства интернета вещей и т.п.). Таким образом уязвимость компьютерной сети становится равной уязвимости самого слабого ее узла.
2. Критически важные централизованные ресурсы сети становятся более уязвимыми для различного рода атак: удаления информации, отказа от обслуживания, контаминацией недостоверной информацией.
3. Среди пользователей компьютерной сети обычно присутствуют люли разной степени подготовленности и организованности, которые могут непреднамеренно (например, посредством социальных фишинговых технологий), а иногда и намеренно способствовать утечкам информации из сети или несанкционированному проникновению в сеть.

Для решения указанных проблем могут быть использованы различные типы организации компьютерных сетей, например, как уже упоминалось, разделение на открытый и закрытый контуры с шлюзами между ними. Необходимость открытого контура связана с наличием внешних неавторизованных пользователей и необходимостью использовать внешние

информационных источники, в том числе зарубежные, например, по сейсмическим и метеорологическим данным, термическим точкам или предупреждения о цунами.

6.1 Организация компьютерных сетей

Для описания взаимодействия устройств в локальных и глобальных компьютерных сетях используются две основные модели:

- OSI (Open System Interconnection) – 7 уровней организации;
- TCP/IP (Transmission Control Protocol/Internet Protocol) – 4 уровня.

Каждый из уровней имеет свои особенности или протоколы передачи и инициации соединений, которые могут быть использованы злоумышленниками для атак (см. следующий раздел).

Таблица 6.1 – Уровни организации сети по системе OSI.

№	Уровни модели OSI	Описание уровня и используемые протоколы
L7	Прикладной	На этом уровне работает прикладное программное обеспечение, например, мессенджер отправляет текстовое сообщение или браузер – запрос на веб-сервер. *Устройства:* Программы – браузеры, мессенджеры, почтовые клиенты и т.п. *Протоколы:* HTTP(S), (S)FTP, WS(S), SMTP, APIs
L6	Представления	На этом уровне производится представление данных в различных форматах: их кодирование, шифрование и, при необходимости сжатие.
L5	Сеансовый	Сеансовый уровень управляет *сессиями*, *сеансами связи* или *соединениями*. На этом уровне данные имеют уже привычный для пользователя вид, например, в виде файла, но необязательно. Сеансы устанавливаются, в частности, для аудио или видеозвонков.
L4	Транспортный	*Протоколы:* TCP, UDP TCP (Transmission Control Protocol) – отправляет данные большими пакетами, разбивая их на сегменты, при этом проверяет корректность доставляемых данных, например, с помощью

		контрольных сумм. TCP работает существенно медленнее UDP (User Datagram Protocol), используемый для передачи аудио или видео, где небольшие потери некритичны.
L3	Сетевой	В полях данных Ethernet-кадров канального уровня записаны IP-пакеты, которые тоже содержит адреса отправителя и получателя, но уже в IP-формате. На сетевом уровне определяются маршруты в сети для данных и логическая адресация в отличии от физической адресации пакетов на предыдущих уровнях *Устройства:* маршрутизаторы, роутер. Маршрутизаторы строят маршруты для пакетов по MAC-адресам, но уже в пределах IP-сети и ее подсетей. *Протоколы:* IP, ARP ARP (Address Resolution Protocol) нужен чтобы конвертировать MAC-адреса в IP-адреса, соотношения записаны в ARP-таблице
L2	Канальный	Потоки сигналов разбиваются на фреймы (кадры), состоящие из MAC-адреса[2] отправителя и получателя, и данных. Может проверяться целостность пакетов данных и исправлять ошибки. *Устройства:* коммутаторы, мосты – передают пакеты только по тому порту, где зарегистрирован MAC-адрес получателя пакета *Протокол:* PPP
L1	Физический	Прямая передача электрического, оптического или радиосигнала. *Устройства:* концентраторы, репитеры *Протоколы:* Ethernet, 802.11 Wi-Fi, GSM, Bluetooth и др.

[2] MAC (Media Access Control) – уникальный для каждого сетевого устройства, включая даже умные лампочки, шестибайтный номер, назначаемый производителем. Например, в шестнадцатеричной записи ea:93:e8:0c:de:b2. В Линукс системах MAC-адрес можно узнать командой ifconfig, в Windows – ipconfig.

TCP/IP – более простая модель, состоящая из 4 уровней, которые соответствуют уровням OSI, как показано в Таблице 6.2. TCP/IP является также стеком (взаимосвязанным набором) протоколов для сети Интернет.

Таблица 6.2 – Соответствие уровней моделей TCP/IP и OSI.

Уровни модели TCP/IP	№ уровня OSI	Уровни модели OSI
Прикладной	L7	Прикладной
	L6	Представительский
	L5	Сеансовый
Транспортный	L4	Транспортный
Межсетевой	L3	Сетевой
Доступ к сети	L2	Канальный
	L1	Физический

В следующем разделе будут рассмотрены вопросы кибербезопасности при работе в компьютерных сетях.

6.2 Классификация угроз в компьютерных сетях

Для систематизации и классификации источников угроз можно использовать обе описанные модели организации сети (Таблица 6.3).

Таблица 6.3 – Уровни организации сети и типы атак.

Типы атак	Уровни модели OSI	Уровни модели TCP/IP
SQL-inj, RCE, LFI, XSS, CSRF, XXE, Malware attack, SSL/TLS Session MITM, Telnet & FTP MITM, HTTP request smuggling	Прикладной Представительский Сеансовый	Прикладной
TCP-SYN, TCP-RST, TCP-ACK, Port scanning	Транспортный	Транспортный
IP/Port Packet MITM, UDP/TCP flood	Сетевой	Межсетевой
MAC flooding, TCP/ARP/DNS spoofing, VLAN hopping, MAC address spoofing, STP spoofing	Канальный	Доступ к сети
Физическое воздействие (повреждение физического канала)	Физический	

Рассмотрим вопросы безопасности, связанные с бесконтрольным доступом к локальной вычислительной сети (ЛВС или LAN) организации.

Уровень доступа к сети. С точки зрения рядовых пользователей, следующие действия на уровне доступа к сети могут привести к компрометации ЛВС организации:

Подключение к внутренней сети организации чужого компьютера (например, через свободный Ethernet-разъем или Ethernet-разъем, предназначенный для другого компьютера).

Как следствие:

- Посредством TCP/ARP-spoofing атаки злоумышленник может связать свой MAC-адрес с легальным IP-адресом, получая доступ к любым данным, отправленным на легальный IP-адрес внутри сети.
- Возможны также атаки типа «UDP/TCP flood» сетевого уровня, для перегрузки сервера сети, при отправке большого количества неподтверждаемых заявок на подключение. Обычно сервер защищен от внешних таких атак межсетевым экраном, атаки изнутри сети делают его уязвимым.

Способом предотвращения является привязка физических портов на маршрутизаторе к MAC-адресам[3] оконечных устройств, это способ используется также Интернет-провайдерами. Существует также обход этой меры: MAC-spoofing – подмена MAC адресов.

Если в проводной сети, правильно настроенный маршрутизатор не позволяет устройству с неправильным MAC-адресом сканировать информационно пакеты в сети, то в сети WI-FI это возможно делать, в том числе, находясь вне зоны контролируемого доступа лиц, например, на улице вне здания или за периметром охраняемой территории, в зависимости от силы сигнала.

Существует дистрибутив Linux – Kali Linux на основе Debian со специально установленными программами для сканирования локальной сети на уязвимости. Он предназначен для специалистов по безопасности, но может использоваться и злоумышленниками.

Транспортный уровень. Предположим, что пользователь запустил у себя на компьютере, например, FTP-сервис для передачи для файлов внутри сети или

[3] MAC-адреса можно изменять даже штатными методами, как, например, в домашних роутерах или в системе Linux с помощью команд iproute2 или macchanger.

службу Telnet для удаленного доступа к другому компьютеру. Это означает, что на транспортном уровне, в сети становятся видны так называемые открытые порты[4] под номерами 21 и 23, соответственно. Обычно при сканировании посылаются запросы на все порты с номера от 0 до 65535 на все компьютеры внутренней сети (SYNC scan), при этом по ответам часто можно определить:

- работающие сетевые сервисы,
- пользователей, которые запустили сервисы,
- допускается ли неавторизованный (анонимный) доступ,
- какие сетевые сервисы используют авторизацию,
- используется ли firewall-защита и др.

Для сканирования на транспортном уровне может использоваться как компьютер как с уже упомянутым дистрибутивом Kali Linux, так и отдельные программы, установленные на пользовательском компьютере, вроде анализатора сетевых пакетов Wireshark.

Основным способами предотвращения являются:

- использование файерволов – программ на маршрутизаторах или устройств в сети, не пропускающих сканирующие пакеты и ведущих регистрацию таких попыток;
- профилактическое сканирование внутренней сети на имеющиеся уязвимости.

6.3 Контрольные вопросы

1. В чем состоят преимущества компьютерных сетей как средства передачи информации по сравнению с материальными носителями? Какие у сетей есть недостатки?
2. Что такое API?
3. Какие два вида уровней организации сети можно использовать для классификации источников опасности?
4. Какой протокол используется на физическом уровне (L1 OSI) в локальной вычислительной сети?

---

[4] Здесь имеется ввиду не физический порт – как на роутере, а «программный» – то есть при отправке на сканируемый компьютер TCP или UDP пакета с некоторым номером от 0 до 65535, скажем 23, компьютер-получатель может вернуть подтверждающий пакет, это означает, что порт 23 (Telnet) «открыт» – то есть на получателе запущена программа, готовая обрабатывать пакеты с такими номерами.

5. На основе какого стека протоколов строится глобальная сеть Интернет?
6. Сколько уровней содержит классификация OSI? TCP/IP?
7. Зачем организуются открытый и закрытый контуры сети? Могут ли они связываться? Как?
8. Что такое MAC-адрес? Должен ли он быть уникальным? Для чего – компьютера в локальной сети? Любого сетевого устройства?
9. Можно ли подменить MAC-адрес?
10. Безопасно ли бесконтрольное подключения сторонних людей, например, гостей на дне открытых дверей, к Ethernet-розеткам ЛВС организации?
11. В чем заключается атака TCP/ARP-spoofing? Как ее можно инициировать?
12. В чем заключается атака UDP/TCP-flood? Как ее можно инициировать?
13. В чем состоит атака MAC-spoofing? Как ее можно инициировать? Какие используются методы противодействия таким атакам?
14. Чем опасно сканирование портов? Стоит ли держать открытыми неиспользуемые сетевые сервисы или порты?

7. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

Защита информации в индустрии информационных технологий выросла в самостоятельную отрасль, требующую специализированных программных и аппаратных средств и подготовленных специалистов. По мере интеграции информационных технологий во все сферы человеческой деятельности, включая государственное управление, банковскую сферу, автоматизированные технологические процессы предприятий, «умные» дома и города, цена взлома и компрометации информационных систем многократно возрастает. Если раньше это относилось только к материальным потерям (потеря клиентов из-за «отказов в обслуживании», простои из-за вирусов-шифровальщиков и платежей вымогателям, несанкционированные банковские трансферы, нарушения в работе и разрушения технологической инфраструктуры), то с развитием беспилотных авиационных систем (БАС) и «интернета вещей» (IoT), опасности могут подвергаться жизнь и здоровье граждан.

Приведем несколько иллюстрирующих примеров:

- Атака с помощью вируса Stuxnet была проведена на атомный объект Ирана, занимающийся обогащением урана, через зараженное USB-устройство (флэшку), по одним данным – непреднамеренно, по другим – завербованным сотрудником центра. Вирус был разработан для работы с промышленными контроллерами фирмы Сименс и намеренно вызывал нерасчетные режимы работы обогатительных центрифуг, управляемых такими контроллерами. В результате заражения целые каскады центрифуг были повреждения или разрушены, что привело к задержкам в осуществлении ядерной программы Ирана [46].
- Группировка Dark River (это может быть самоназвание или условное название, выбранное экспертами по безопасности), целенаправленно атакует предприятия российского оборонного комплекса, используя сложную модульную бэкдор[5]-программу, которая может незаметно действовать в скомпрометированной инфраструктуре в течение долгого времени с целью шпионажа и кражи конфиденциальной информации. В настоящее время известно несколько случаев применения MataDoor в

[5] Бэкдор (от англ. back door – «черный ход») – вредоносная программа или намеренно оставленная лазейка в легальном программном обеспечении, предоставляющая доступ к устройству для несанкционированных действий.

кибератаках, все они были нацелены на крупные организации, связанные с оборонно-промышленным комплексом. Бэкдор маскируется: имена его исполняемых файлов похожи на названия легального ПО, установленного на зараженных устройствах, а ряд образцов имеет действительную цифровую подпись, разработчики использовали различные виды утилит-упаковщиков, скрывающих вредоносный код. Основной канал распространения: внедрение бэкдора начинается с фишингового[6] письма, к которому злоумышленники прикрепляют документ в формате DOCX, посвященный сфере деятельности атакованного предприятия. Бэкдор побуждает получателя включить режим редактирования документа (просто открыть вложение недостаточно) для отработки для отработки известного эксплойта уязвимости CVE-2021-40444. Похожие письма рассылались на российские предприятия ОПК в августе-сентябре 2022 года. Чтобы побудить пользователя включить режим редактирования, в тексте документа намеренно использовался неконтрастный шрифт. Чтобы его прочитать, пользователь менял цвет шрифта, запуская режим редактирования. Одновременно с этим происходила загрузка и выполнение вредоносной полезной нагрузки с контролируемого киберпреступниками ресурса [47].

- Из недавних примеров, государственные организации из России и Белоруссии подверглись атаке новой хакерской группировки – Sticky Werewolf («Липкий оборотень»). Атакам подвергались: администрация Красноярского края, Брестский исполнительный комитет, и были зафиксированы фальшивые исковые документы от имени Савеловского суда. Атаки используют социальную инженерию[7] в совокупности с коммерческими вредоносными программными средствами (доступными в Даркнете). При атаке госорганизация получают вредоносный документ, с помощью которого происходит заражение ПК. Группировка активна минимум с апреля и совершила более 30 атак. Ссылки для мошеннических писем создаются с помощью сервиса IP Logger. Он позволяет собирать

[6] Фишинг (англ. phishing, созвучно англ. fishing – «рыбная ловля») – использование фейковых электронных писем, сайтов, приложений для получения личных данных, паролей, номеров кара, банковских счетов или другой конфиденциальной информации.

[7] Социальная инженерия (social engineering) – совокупность психологических и социологических приемов, методов и технологий, позволяющих выманить конфиденциальную информацию у жертвы или вынудить ее к нежелательным действиям.

информацию о кликнувших пользователях: время перехода, IP-адрес, страну и город, версию браузера и операционную систему, это помогает Sticky Werewolf отсеять системы, которые не представляют для них интереса, и сосредоточить атаки на наиболее приоритетных. Кроме того, с IP Logger группировка может использовать собственные доменные имена при создании ссылок, чтобы адреса не выглядели подозрительно [48].

Отметим различия между терминами «информационная безопасность» (синонимы – «защита информации», «ИТ-безопасность») и «кибербезопасность». Информационная безопасность демонстрирует более комплексный подход к обеспечению защиты данных, чем непосредственно кибербезопасность. Например, если за пределами организации произошла кража флэшки с незашифрованными служебными документами, то инцидент относится к сфере информационной безопасности, а не к сфере кибербезопасности.

В теории информационной безопасности меры защиты информации разделяются на:

- *Технические* – средства защиты от несанкционированного доступа, доверенной загрузки компьютерных устройств, межсетевые экраны, антивирусы, системы обнаружения вторжения, средства контроля и анализа защищенности, резервного копирования и восстановления информации, защиты среды виртуализации, криптографические средства, по большинству из этих средств требуется сертификация ФСТЭК. Перечень сертифицированных средств содержится в соответствующем реестре, например, [49].
- *Организационные* – внутренние положения, регламенты и процедуры в дополнение к федеральному законодательству, штатные должности специалистов, журналы учета средств хранения информации и т.п., например, статья 18.1 № 152-ФЗ обязывает оператора персональных данных (ПДн) – юридическое лицо:
  - назначить ответственного за организацию обработки ПДн – издание соответствующего приказа или распоряжения;
  - издать политику в отношении обработки ПДн;
  - ознакомить и (или) обучить работников, осуществляющих обработку ПДн, с требованиями по защите ПДн;
  - обеспечить неограниченный доступ к политике в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн (публикация на сайте организации, если он есть).

Дополнительно, пункт 2 ст. 19 обязует оператора применять организационные меры согласно Постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также:

  - определить угрозы безопасности ПДн, то есть составить модель угроз;
  - вести учет машинных носителей ПДн – разработать и вести журналы учета;
  - установить правила доступа к персональным данным, например, вести журнал учета допущенных к обработке ПДн;
  - обеспечить регистрацию и учет действий, совершаемых с персональными данными в информационной системе.

- *Физические* – выделенные помещения, железные двери, замки, сигнализация, жалюзи, датчики доступа и присутствия, экраны, сейфы, охрана, видеонаблюдение, биометрические средства защиты, желательно не зависящие от защищаемой информационной сети.

Таким образом, кибербезопасность сосредоточена только на технических мерах защиты, а информационная безопасность – на всех трех аспектах.

В заключение введения, приведем 10 непреложных правил, которым рекомендует следовать компания Микрософт [50].

10 НЕПРЕЛОЖНЫХ ПРАВИЛ КИБЕРБЕЗОПАСНОСТИ

Правило 1: если злоумышленник убедил тебя запустить его программу на твоем компьютере, это уже не совсем твой компьютер.

Правило 2: если злоумышленник может подправить операционную систему у тебя на компьютере, это уже не твой компьютер.

Правило 3: если у злоумышленника есть свободный доступ к твоему компьютеру, это уже не твой компьютер.

Правило 4: если злоумышленнику удалось запустить активный контентна твоем веб-сайте, это больше не твой веб-сайт.

Правило 5: слабые пароли побеждают сколь угодно сильную защиту.

Правило 6: защита сети и компьютера настолько надежна, насколько надежен системный администратора.

Правило 7: зашифрованные данные надежны не более, чем ключ расшифровки.

Правило 8: просроченные базы антивируса, только маржинально лучше, чем никакого антивируса.

Правило 9: абсолютная анонимность практически недостижима, ни онлайн, ни оффлайн.

Правило 10: технология не панацея.

Контрольные вопросы

1. Как действует бэкдор-программа?
2. В чем заключается фишинг?
3. В чем заключаются методы социальной инженерии?
4. Мошенник представляется сотрудником службы безопасности банка и предлагает срочно ввести код из СМС для спасения средств на счету. Каким методом пользуется злоумышленник?
5. Имея сложности с доступом к своему счету с криптокойнами, пользователь скачал с сайта в интернете программу для доступа к другой криптовалюте, которая, согласно рекламе на сайте, должна помочь с доступом и к его активам. После попытки ее использования пользователь обнаружил, что все криптокойны с его кошелька исчезли. Какой технологией воспользовались мошенники?
6. Перечислите виды мер защиты информации.
7. В чем состоят технические меры защиты информации?
8. В чем могут состоять организационные меры защиты информации?
9. Что может относиться к физическим средствам защиты информации?
10. В чем отличия между кибербезопасностью и информационной безопасностью?

7.1 Направления угроз (вектора атак)

Как видно, направления информационной защиты в индустрии информационных технологий является сложной областью, с развитой системой регулирования и требует для работы привлечения высокопрофессиональных специалистов. Тем не менее существует ряд направлений, которые требует от конечных пользователей соблюдения правил информационной «гигиены».

Одно из недавно возникших направлений утечки информации – это использование чат-ассистентов на основе больших языковых моделей (LLM – Large Language Models, англ.), наиболее громко прозвучавший представитель: ChatGPT, на основе LLM-моделей GPT3, GPT3.5, GPT3.5-turbo, GPT4, GPT4-

turbo) компании OpenAI, к которой в настоящее время подключились и другие крупные компании, например, компания Google с Google Bard и др.

При использовании этих систем, для помощи в составлении служебных и особенно конфиденциальных документов вводимая информация отправляется на внешние сервера и может быть перехвачена или специально извлечена. Кроме того, если в применяемой LLM пользовательские данные используются для дообучения модели, то переданные данные могут в последствии всплывать в последующих запросах других пользователей, с подходящим языковым контекстом.

7.2 Подходы к управлению информационной безопасностью

С точки зрения управления безопасностью для защищаемой информации должны быть обеспечены три условия (ISO/IEC 27001:2013):

1. *Конфиденциальность* – гарантия, что никто не сможет получить к информации несанкционированный доступ.
2. *Целостность* – информация не может быть изменена без ведома владельца.
3. *Доступность* – возможность для владельца информации получить неограниченный доступ к ней.

Иногда еще добавляют условие авторизуемости (accountability) – возможность проверить откуда появилась информация.

Для достижения этих условий создана целая индустрия ИТ-безопасности, полный обзор которой выходит за рамки данного пособия. Рассмотрим только основные концепции, применяемые на практике.

Выделяют следующие разделы (домены) информационной безопасности (с пояснениями):

Проектирование безопасности (Security Engineering)

Процесс проектирования безопасности концепция обеспечения ИБ, обследование информационной инфраструктуры, оценка информационных активов и рисков, политики, положения и процедуры, инструкции для персонала, планы аудита

Персонал и квалификация наличие штатных должностей, связанных с обеспечением ИБ, компетентных специалистов, непрерывная систем повышения квалификации

Управление процессом проектирования безопасности регулярные ревизия и пересмотр политик, положений, внутренних процессов, с учетом новых угроз и практики применения

Практики общего управления действующие политики, положения, процедуры, регламенты, наличие ответственных лиц и т.д.

Облачная безопасность набор политик, программных и технологических средств контроля и технологий для защиты данных, приложений и инфраструктурных облачных сервисов – выделяется в отдельную категорию ввиду особой важности облачной инфраструктуры в современных условий и большей уязвимости облачных информационных систем в отличии от внутренних сетей, где возможно задействовать дополнительные средства контроля доступа, например, физические

Контроль доступа (IAM/PAM) идентификация пользователей (IAM – Identity Access Management), управление привилегированным доступом к критически важным информационным ресурсам (PAM – Privileged Access Management) – регистрация новых пользователей, предоставление и отзыв прав доступа, актуализация на основе кадровых событий

Криптографические средства программы или устройства, для шифрования документов или передаваемой информации, или генерации электронной подписи – криптографические средства сертифицируются

Интеграция систем объединение различных систем безопасности: доступа, системы видеонаблюдения, пожарной безопасности, пожаротушения, последние физически влияют на информационную безопасность данных

Безопасная архитектура стратегические решения по построению информационных систем (какие продукты и каких производителей использовать), политикам и используемым технологиям для защиты информационных активов

Операции безопасности (Security Operations – SecOps)

Основы политики, положения, штатные единицы системных администраторов, специализирующихся на информационной безопасности

Инструменты и процедуры системы отслеживания вторжений, системы двухфакторной авторизации, проверка на защищенность паролей пользователей и т.п., интеграция с процедурами организации

Процесс (PDPR – Personal Data Protection Rules, IR – Incident Response) защита персональных данных сторонних пользователей информационной системы организации, реагирование на инциденты безопасности

Персонал и квалификации системные администраторы, специализирующиеся на информационной безопасности, их квалификация, сертификация, непрерывная (ежегодная) система повышения квалификации

Предотвращение обеспечение безопасности службы доменных имен (DNS), для предотвращения подмены интернет адресов; непрерывный мониторинг сети организации и немедленная реакция на подозрительные события; обработка ложных срабатываний; сопровождение интерактивных атак; мониторинг уязвимости данных; мониторинг сетевых протоколов на уровне пакетов данных, затруднен при использовании vpn-соединений

(необходимы, в первую очередь, для установления безопасной связи между распределенным локациями организации) и современных сетевых протоколов вроде https – в полной мере реализуется при круглосуточной работе центра, что возможно только для больших организаций или ведомств целиком

Выявление вторжений использование индикаторов атак (IoA), анализ тактик, техник и процедур злоумышленников (TTP), поддержание «белых» и «черных» списков активностей и шаблонов исключений, настройка правил детектирования атак; в последнее время активно используются алгоритмы машинного обучения

Защита предотвращение или ограничение, за счет оперативного вмешательства, времени доступа злоумышленника к ценным информационным активам организации

Восстановление (DR – Disaster Recovery, BCP – Business Continuity Planning) способность организации реагировать на и восстанавливать деятельность после инцидента безопасности

Управление уязвимостями постоянный, активный и часто автоматизированный процесс проверки на известные уязвимости и применение корректирующих обновлений безопасности

Реакция на инциденты внутренне информирование и при необходимости публичное оповещений о инцидентах безопасности; купирование и устранение последствий; расследование

Цифровые следы активные и пассивные – данные, оставляемые пользователем при посещении сайтов в интернете, социальных сетях, онлайн формах, или собираемые без его ведома

Активная защита набор тактик, направленных на раннее выявление вторжений, например, путем создания контролируемых уязвимостей или фальшивых активов, тактики могут включать встречное вторжение в информационную систему злоумышленника

Предотвращение утечек данных (DLP – Data Leak Prevention) технологии предотвращения утечек конфиденциальной информации, а также программные и программно аппаратные средства предотвращения утечек

Менеджмент информации и событий безопасности (SIEM) собирает данные журнала событий от различных источников, анализирует их в реальном времени, выявляя аномальные действия, и принимает необходимые меры

Центр управления безопасностью (SOC – Security Operation Center) отвечает за круглосуточный мониторинг и оперативное расследование потенциальных угроз кибербезопасности, имеет смысл только для крупных организаций или ведомств целиком

Государственное и отраслевое регулирование (Governance)

Основы общая оценка регулятивного влияния, например, в части обращения с персональными данными; политики п процессы актуализации внутренней нормативной базы согласно изменениям во внешнем регулировании

Нормы – ведомственные отслеживание изменений ведомственной нормативной базы: приказы, рекомендации, регламенты

Нормы и законы – государственные отслеживание изменений в государственной законодательной базе, нормативной базе регулирующих органов

Контрольные списки (WSP – Written Supervisory Procedures) комплекты документов, касающиеся политик, персонала, процедур безопасности для регулирующего органа

Аудит соответствия обычно внешняя, добровольная или обязательная проверка на соответствие техническим и законодательным нормам

Оценка рисков

Основы наличие внутренних политик, положений и процедур организации, касающихся оценок риска информационной безопасности

Инструменты и процедуры выполнение этапов идентификации активов (сетей, подсетей, серверов, операционных систем, приложений, баз данных, программных инструментов), создание профиля риска для каждого актива, снижения риска для каждого информационного актива, путем выполнения организационных и технических процедур

Персонал и квалификация наличие квалифицированного (и желательно сертифицированного персонала[8]) и выделенных должностей

Сканирование на уязвимости информационной инфраструктуры постоянный и регулярный углубленный мониторинг внутренней сети на несанкционированное подключение устройств, открытых программных портов, подозрительной активности программного обеспечения

Сканирование используемого исходного программного кода используется при наличии собственной программной разработки, для исключения заражения кода, используемого для конечного программного обеспечения

Оценки безопасности данных отдельная оценка риска для данных организации, включая классификацию по важности, процедуры регулярного сохранения (бэкапа) и оперативного восстановления

Риски от сторонних компонент при анализе и визуализации внутренних данных, например, широко используются сторонние свободно распространяемые программные пакеты, которые могут оказаться как специально (хактивизм), так и непреднамеренно зараженными

Проверки на вторжения практики условно атакующей (красной) команды, практики защищающейся (голубой) команды и их совместной (фиолетовая команда) работы

[8] Пока не существует независимой российской системы сертификации специалистов по кибербезопасности взамен той, которая была у ушедших зарубежных коммерческих вендоров.

Физическая безопасность и безопасность территории (Physical and Environmental Security)

Основы контроль доступа на территорию, санкционированный доступ к помещениям, наличие систем видеонаблюдения и т.д.

Безопасность «интернета вещей» наличие «умных устройств», умных ламп, умных электро- и теплосчетчиков, иногда требуемых по закону, выключателей и переключателей, часто иностранных производителей и еще чаще с зарубежными компонентами, создают дополнительные, трудно распознаваемые и плохо контролируемые угрозы информационной безопасности организации, ввиду нерегулярных обновлений безопасности, исчезновения вендоров или злонамеренного использования

Работа с кадрами: осведомленность (HR Awareness & Security)

Основы наличие политик по повышению осведомленности пользователей о угрозах информационной безопасности

Тренинги регулярные занятия, методические материалы, курсы повышения квалификации

Программа повышения осведомленности процедуры для реализации вышеупомянутых политик повышения осведомленности

В дополнение рассматривают еще домен «Безопасной разработки программного обеспечения», если организация ведет такую разработку.

Особое внимание в законодательстве России уделяется безопасности объектов критической информационной инфраструктуры, которая регулируется Федеральным Законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который вступил в силу с 1 января 2018 года. Кроме подписания данного Закона о КИИ, были назначены федеральные органы исполнительной власти (ФОИПВ), отвечающие за реализацию норм данного закона. Так, Федеральная служба по техническому и экспортному контролю (ФСТЭК) России была назначена уполномоченным ФОИВ в области обеспечения безопасности критической информационной инфраструктуры РФ. На Федеральную Службу Безопасности (ФСБ) РФ были возложены функции обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (далее – система ГосСОПКА). ГосСОПКА – выполняет функции центра мониторинга информационной безопасности (Security Operations Center, SOC) в государственном масштабе.

7.2.1 Контрольные вопросы

1. Какие три условия должны быть выполнены для обеспечения безопасности информации?
2. В чем заключается конфиденциальность, целостность, доступность информации?
3. Перечислите 6 основных доменов информационной безопасности.
4. Постройте 6 основных доменов информационной безопасности в порядке их важности для государственной организации? Обоснуйте выбранный порядок.
5. В чем заключается проектирование безопасности организации?
6. Чем занимаются сотрудники ситуационного центра информационной безопасности?
7. Как учитывается государственное и отраслевое регулирование информационной безопасности в деятельности организации?
8. В чем заключается оценка рисков информационной безопасности?
9. В чем заключается физическая безопасность и как физическое обеспечение безопасности территории влияет на информационную безопасность организации?
10. Укажите основное направления работы с кадрами для повышения информационной безопасности организации.
11. Каким законом регулируется безопасность критической информационной инфраструктуры (КИИ)?
12. Что относится к объектам КИИ?
13. Какие три условия должны быть выполнены для обеспечения безопасности информации?
14. Что такое систем ГосСОПКА?

7.3 Кибербезопасность в операционных системах семейства Linux

Магистральное направление повышения информационной безопасности в России со стороны конечных пользователей состоит в переходе на сертифицированные отечественные операционные системы на основе ядра Linux (ALT Linux, Ред ОС, ROSA Linux и др., в системе МЧС России – это Astra Linux). До перехода на сертифицированные системы настройка используемых Linux-систем должна осуществляться в соответствии с рекомендациями ФСТЭК [51].

Часть из этих настроек относиться к пользовательскому пространству и может быть проверена конечным пользователем.

Основные понятия, команды и исполняемые скрипты (программы для настройки и обслуживания системы) Линукс, необходимые для понимания рекомендаций:

- **Операционная система Линукс, ОС Линукс, Линукс система** – программа на основе свободно распространяемого кода ядра Linux, которая управляет работой компьютера. Компьютеры, использующие ОС Линукс, будут основными в защищенных информационных системах.
- chmod (change mod – изменение режима) – программа для изменения прав доступа к файлам и каталогам, права записываются одно строкой для трех типов пользователей:
  - владельца файла (u – *user*)
  - для пользователей, входящих в группу владельца (g – *group*)
  - для других пользователей (o – *other*)

  Пример: Права «rwxr-xr--» устанавливаются командой:

  chmod 751 filename

	владелец **u**ser	группа **g**roup	остальные **o**ther
буквенная запись	rwx	r-x	r--
read	1	1	1
write	2	-	-
e**x**ecute	4	4	-
восьмеричная запись (сумма)	7	5	1
описание	пользователь может читать, записывать и исполнять	члены группы могут читать и исполнять, но не записывать	остальные пользователи могут только читать

  Здесь:
  - право на чтение (r) всегда добавляет 1 в итоговую сумму,
  - право на запись (w) всегда добавляет 2 в итоговую сумму,
  - право на исполнение (x) всегда добавляет 4 в итоговую сумму.

  1, 2, 4 – последовательные степени двойки, если право не предоставляется, то в буквенной записи ставится прочерк, а в сумму ничего не добавляется

(или, по-другому, добавляется 0). Для папки право на исполнение означает право ее, папку, открыть.

- `su` (Super User – суперюзер или суперпользователь) – привилегированный пользователь системы Линукс, имеющий доступ ко всем ресурсам компьютера. Один и тот же человек, обычно это администратор системы, может входить в систему как обычный пользователь, так и как суперпользователь.
- Команда `sudo` (SUperuser DO – выполнить с привилегиями суперпользователя) – выполняет команды Линукс с привилегиями суперопользователя, запрашивая при этом дополнительный пароль. Эта команда может использоваться для выполнения, критически важных с точки зрения безопасности системы, действий: команд настройки системы, задания прав доступа к файлам, папкам и другим ресурсам компьютера (сетевым интерфейсам и т.п.), может использоваться для просмотра системных файлов (какие пользователи, с какими правами есть в системе, какие сетевые протоколы открыты), для добавления новых пользователей. Права на выполнения этой команды должны выдаваться с особой осторожностью (пп. 2.2.1, 2.2.2).
- `SSH` (Secure SHell protocol) – протокол безопасной оболочки, позволяет, используя криптографию для авторизации и шифрования сообщений, безопасно пересылать команды на другой компьютер через небезопасную сеть (Интернет), в частности позволяет выполнять работы по обслуживанию системы в терминале (текстовой оболочке) из удаленного компьютера. Очень удобен и поэтому любим администраторами систем, потому что позволяет быстро исправлять проблемы в настройках из любого места и в любое время (из дома, ночью, из отпуска), для поддержания системы в работоспособном состоянии 24/7, то есть 24 часа в сутки 7 дней в неделю. Однако при компрометации (завладении личным компьютером или паролями) этот протокол несет критические риски для администрируемой системы, поэтому запрещен (п. 2.1.2). Практика показывает, что проблемы безопасности, связанные с привычками или удобством людей, являются одними из самых трудноустранимых.

Приведем ряд положений из рекомендаций ФСТЭК [51] (нумерация пунктов сохранена), с комментариями:

2.1. Настройка авторизации.

В операционной системе Linux необходимо:

2.1.1. Не допускать использование учетных записей пользователей с пустыми паролями.

Настроить учетные записи таким образом, чтобы каждый пользователь системы либо имел пароль, либо был заблокирован по паролю. В системах Linux данную возможность обеспечивает файл /etc/shadow.

2.1.2. Обеспечить отключение входа суперпользователя в систему по протоколу SSH путем установки для параметра PermitRootLogin значения no в файле /etc/ssh/sshd_config (Рисунок 7.1).

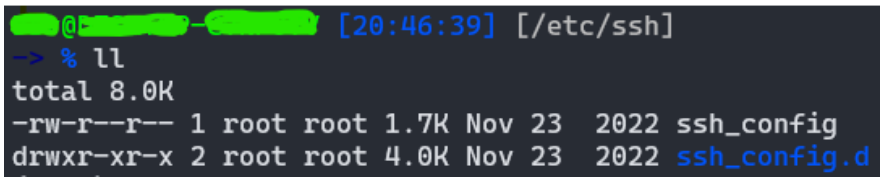

Рисунок 7.1. – Местоположение файла настроек ssh-соединения.

d – перед буквенной строкой прав доступа второй записи означает, что это папка (d – directory). Видно, что файлы и папка принадлежат root (su), но зайти и посмотреть может любой пользователь.

2.2. Ограничение механизмов получения привилегий

При ограничении механизмов получения привилегий необходимо:

2.2.1. Обеспечить ограничение доступа к команде su путем добавления в файл /etc/pam.d/su следующей строки:

auth required pam_wheel.so use_uid

Задать список пользователей в записи для группы wheel в файле /etc/group:

wheel:x:10:root,<user list>

2.2.2. Ограничить список пользователей, которым разрешено использовать команду sudo и разрешенных к выполнению через sudo команд путем пересмотра файла /etc/sudoers.

2.3. Настройка прав доступа к объектам файловой системы

При настройке прав доступа к объектам файловой системы необходимо:

2.3.1. Установить корректные права доступа к файлам настройки пользователей, а именно к файлам с перечнями пользовательских идентификаторов (/etc/passwd) и групп (/etc/group), либо хранилищам хешей паролей (в операционных системах GNU/Linux, Solaris, HP-UX: /etc/shadow, AIX: /etc/security/passwd), с помощью команд:

chmod 644 /etc/passwd – запрет записи в файл паролей /etc/passwd всем, кроме владельца – суперпользователя, чтение для остальных пользователей допускается, потому что пароли необходимы для подтверждения прав и все равно хранятся в зашифрованном виде;

chmod 644 /etc/group – запрет записи всем, кроме владельца – суперпользователя, в файл задания групп пользователей /etc/group (и назначения групповых привилегий);

chmod go-rwx /etc/shadow – запрет записи всем, кроме владельца – суперпользователя.

2.3.2. Установить корректные права доступа к файлам запущенных процессов путем выполнения команды вида:

chmod go-w /путь/к/файлу

для всех исполняемых файлов, запущенных в настоящий момент, и соответствующих библиотек. После этого необходимо осуществить проверку, что директория (папка), содержащая данный файл, а также все родительские директории недоступны для записи непривилегированным пользователям.

2.3.3. Установить корректные права доступа к файлам, выполняющимся с помощью планировщика задач cron неавторизованными пользователями путем выполнения команды

chmod go-w путь_к_файлу (запрет на запись всем кроме пользователя)

для каждого файла (либо команды), который вызывается из заданий cron. В противном случае это может привести к выполнению произвольного кода от имени владельца задания cron (в том числе root, что может привести к полной компрометации системы).

2.3.4. Установить корректные права доступа к файлам, выполняемым с помощью sudo путем изменения владельца командой

chown root путь_к_файлу (сменить владельца на root)

для каждого исполняемого файла, который можно запускать с привилегиями суперпользователя root, но владельцем которого является обычный пользователь и выполнения команды

chmod go-w путь_к_файлу

для каждого исполняемого файла, который можно запускать с привилегиями суперпользователя root и к которому имеют доступ на запись все пользователи.

2.3.5. Установить корректные права доступа к стартовым скриптам системы путем выполнения команды

chmod o-w (запретить другим пользователям запись)

к каждому файлу в директориях /etc/rc#.d (/etc/rc1.dcd /etc/rc2.d, …), а также к файлам .service, присутствующим в системе.

2.3.6. Установить корректные права доступа к системным файлам заданий (конфигурационным файлам) cron при помощи команды

chmod go-wx путь_к_файлу_или_директории.

К системным файлам-описаниям очередей cron относятся следующие файлы (могут присутствовать не всегда, в зависимости от операционной системы и ее настроек, см. рисунок 7.2):

/etc/crontab;
/etc/cron.d (директория и файлы внутри нее);
/etc/cron.hourly (директория и файлы внутри нее);
/etc/cron.daily (директория и файлы внутри нее);
/etc/cron.weekly (директория и файлы внутри нее);
/etc/cron.monthly (директория и файлы внутри нее).

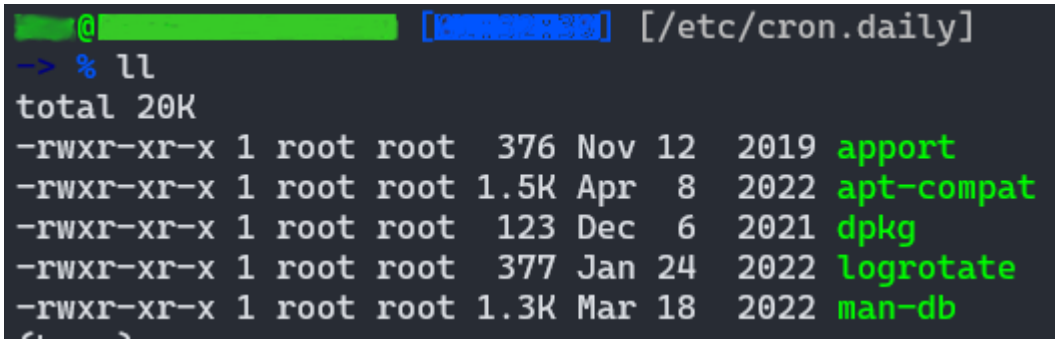

Рисунок 7.2. – Пример содержимого папки /etc/cron.daily.

Эти команды предназначены для ежедневного выполнения с правами root.

2.3.7. Установить корректные права доступа к пользовательским файлам заданий cron при помощи команды вида:

chmod go-w путь_к_файлу_заданий.

2.3.8. Установить корректные права доступа к исполняемым файлам и библиотекам операционной системы путем анализа корректности прав доступа к утилитам и системным библиотекам, расположенным по стандартным путям

(/bin, /usr/bin, /lib, /lib64 и другим путям), а также к модулям ядра (для Linux: /lib/modules/версия-текущего-ядра).

Местоположение большинства стандартных исполняемых файлов указано в переменной $PATH пользователя root.

2.3.9. Установить корректные права доступа к SUID/SGID-приложениям (с правами суперюзера или его группы) путем проведения аудита системы на предмет поиска всех SUID/SGID-приложений – права доступа к каждому из них не должны позволять остальным пользователям изменять его содержимое (в особенности если это SUID-приложение и его владелец root). В противном случае следует выполнить команду вида:

chmod go-w /путь/к/приложению.

Проверить, что среди выявленных SUID/SGID-приложений не присутствуют лишние (например, если определен «белый» список таких приложений), в противном случае следует снять с таких приложений SUID/SGID-биты.

2.3.10. Установить корректные права доступа к содержимому домашних директорий пользователей

.bash_history, .history, .sh_history и т. п. – файлы истории команд оболочек (чтобы другие пользователи не могли увидеть история работы),

.bash_profile, .bashrc, .profile, .bash_logout и т. п. – файлы настройки оболочки (могут устанавливать сокращения для команд и переопределять команды, что можно использовать для обмана пользователя), путем установки на каждый из указанных файлов корректных прав доступа с помощью команды вида:

chmod go-rwx путь_к_файлу

– отмена чтения, записи и исполнения для членов группы кроме владельца и других пользователе.

2.3.11. Установить корректные права доступа к домашним директориям пользователей с помощью команды

chmod 700 домашняя_директория – собственник файлов и папок имеет все права на свои файлы (записи, открытие и исполнение; причем открытие папки с файлами означает ее исполнение).

Домашние директории рядовых пользователей системы обычно расположены в папке /home, например, для пользователя с именем user1, в папке:

/home/user1

Как видно даже из вышеприведенных примеров, администрирование Линукс-системы требует специальной подготовки. Однако знание базовых принципов организации пользовательской среды системы Линукс, таких как наличие иерархии «рядовые пользователи/группы доступа/суперпользователь»; назначение прав доступа к файлам и т.д., позволяет рядовому пользователю системы выявить нарушения протоколов безопасности.

7.3.1 Контрольные вопросы

1. Допускается ли открытие в Линукс-системе гостевого пользователя с пустым паролем?
2. Для каких целей могут использоваться привилегии sudo?
3. Для чего используется протокол ssh? Почему надо заблокировать использование этого протокола?
4. Для каких целей в Линукс системе используется системный скрипт cron? Какие опасности связаны с неконтролируемым использованием этой команды?
5. Что содержится в папках cron.hourly, cron.daily, cron.weekly, cron.monthly? В какой папке они сами находятся?
6. Для чего используется команда chmod?
7. Какие три параметра доступа к объектам файловой системы регулирует chmod? Для каких трех типов пользователей?
8. Какие права устанавливает команда chmod 576 filename?
9. Что делает команда chmod go-rwx путь_к_файлу? chmod go-wx?
10. Какие права устанавливает команда chmod 700 путь_к_файлу?
11. Для чего используется команда chown?

7.4 Операционная система специального назначения Astra Linux

В связи с ограничениями, вводимыми компанией Микрософт в отношении российских коммерческих и государственных заказчиков, фактически единственным путем независимого развития российской информационной отрасли, в том числе и государственного назначения, осталось создание российских дистрибутивов на основе открыто распространяемого программного обеспечения, где практически безальтернативно господствуют дистрибутивы на основе ядра Linux.

Astra Linux – операционная система специального назначения на базе ядра Linux, была создана для нужд органов государственного и военного управления и других учреждений, которые работают с информацией ограниченного доступа. Разработка Astra Linux была начата в 2008 году АО «НПО РусБИТех» при участии Министерства обороны РФ. Встроенные средства защиты ОС разработаны совместно с Академией ФСБ России и Институтом системного программирования РАН. 28 октября 2011 вышел в свет релиз «Смоленск» Astra Linux Special Edition 1.2, а в 2013 году Astra Linux была принята на снабжение Минобороны России.

В конце 2009 года в первые появилась свободно распространяемая версия ОС общего назначения Astra Linux Common Edition релиз «Орел».

Начиная с обновления 1.7, в целях упрощения процесса сертификации, ОС Astra Linux поставляется в виде единого дистрибутива, способного штатно реализовывать любой из 3-х уровней работы подсистемы безопасности (уровне защищенности), реализованном запатентованными средствами защиты информации (СЗИ) (Рисунок 7.3).

Рисунок 7.3. – Уровни защищенности ОС Astra Linux.
(Источник: ГК «Астра»)

Более подробно назначение и функциональные возможности различных уровней защищенности ОС Astra Linux приведены в Таблице 7.1.

Таблица 7.1. Уровни защищенности ОС Astra Linux

Условное наименование	Уровень защищенности	Назначение и функциональные возможности

«Орел»	Базовый	работа с общедоступной информацией в ИТ-системах различных организаций
«Воронеж»	Усиленный|	предназначен для обработки и защиты информации ограниченного доступа, не составляющей государственную тайну, в том числе в ГИС, ИС ПД и значимых объектов КИИ любого класса (уровня) защищенности (категории значимости)
«Смоленск»	Максимальный	обеспечивает защиту информации, содержащей государственную тайну любой степени секретности и предназначен для обработки информации любой категории доступа в ГИС, в ИС ПД, в составе значимых объектов КИИ, в иных информационных (автоматизированных) системах, обрабатывающих информацию ограниченного доступа, в т.ч. содержащую сведения, составляющие государственную тайну до степени секретности «особой важности» включительно

Для реализации ОС «Astra Linux» реализует следующий комплекса средств защиты:

- Модули подсистемы безопасности PARSEC, входящие в состав ядра ОС;
- Библиотеки и модули аутентификации (по требованиям российского законодательства);
- Утилиты безопасности;
- Подсистема протоколирования (регистрации) активности;
- Графическая подсистема (рекомендуется для обычных пользователей) и консольный вход (через терминал) в систему;
- Средства контроля целостности состава системы (работает также против бэкдоров);
- Средства восстановления данных и восстановления исполняемых модулей (работает также против бэкдоров);
- Средства разграничения доступа к виртуальным машинам (необходимы в основном для серверов);
- Средства разграничения доступа к подключаемым устройствам.

Рисунок 7.4. – Комплекс средств защиты ОС Astra Linux.
(Источник: ГК «Астра»)

7.2.1 Контрольные вопросы

1. Является ли Astra Linux полностью российской операционной системой?
2. На каком дистрибутиве Linux основана Astra Linux: RedHat, Ubuntu, Debian?
3. Имеется ли свободно распространяемая версия Astra Linux?
4. Какая версия Astra Linux является основной, специальной, общей?
5. Какая версия Astra Linux подходит для обработки информации степени секретности «особой важности»? Какой уровень защищенности в ней реализован?
6. Какая версия Astra Linux предназначена для работы с общедоступной информацией? Какой уровень защищенности в ней реализован?
7. Какая версия Astra Linux предназначена для работы с информацией ограниченного доступа? Какой уровень защищенности в ней реализован?
8. Какого уровня защищенности Astra Linux достаточно для работы с КИИ любой категории значимости?
9. Какого уровня защищенности Astra Linux достаточно для работы с ГИС?
10. Какого уровня защищенности Astra Linux достаточно для работы с ИС ПДн?

ЗАКЛЮЧЕНИЕ

Динамичное развитие информационных технологий, появление новых технологий обработки больших данных, глубокого обучения, интернета вещей приводит к все большей востребованности достижений информационно индустрии для решения всего спектра задач профилактики, предупреждения, обнаружения, мониторинга и ликвидации ЧС. Еще одним фактором интенсивных изменений в российской отрасли является рост международной напряженности, требующий кардинальной перестройки используемой технологической основы информационных технологий, и сопряженный с новыми рисками вмешательств враждебных высокотехнологичных государственных игроков (акторов) во все более необходимые информационные системы.

Вышеперечисленные факторы и активная позиция МЧС России по внедрению современных информационных технологий в практику ГЗ (гражданской защиты) и ГО (гражданской обороны) требует оперативного обновления методических материалов, используемых при подготовке обучающихся по программам государственного и муниципального управления при изучении соответствующих дисциплин. В настоящем пособии, авторы попытались дать актуальный срез текущей ситуации использования информационных технологий в поддержке принятия решений в чрезвычайных ситуациях, а также показать тенденции изменений, в том числе, в нормативной и законодательной базе.

Поскольку особенностью индустрии информационных технологий является непосредственное вовлечение пользователей в работу информационных систем, часто надежность и безопасность такой системы напрямую зависит от уровня компетентности, дисциплинированности и просто организованности рядового пользователя. Для повышения уровня технической информированности таких пользователей в пособии отдельное внимание уделено базовым принципам работы компьютерных сетей и рабочих станций, понимание которых должно помочь сориентировать пользователя в технологиях, на которых базируются современные информационные системы и программные средства.

СПИСОК ЛИТЕРАТУРЫ

1. Межгосударственный стандарт ГОСТ 22.0.06-2023 «Безопасность в чрезвычайных ситуациях. Источники природных чрезвычайных ситуаций. Поражающие факторы. Номенклатура параметров поражающих воздействий» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 июля 2023 г. № 533-ст) (не вступил в силу)
2. Бурейский феномен [Электронный ресурс] Российское географическое общество. 2019. URL: https://www.rgo.ru/ru/article/bureyskiy-fenomen (дата обращения: 27.08.2023).
3. Постановление Правительства РФ от 21 мая 2007 г. № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера» (с изменениями и дополнениями). [Электронный ресурс]. 2007. URL: https://base.garant.ru/12153609/ (дата обращения: 01.09.2023).
4. Цунами в России. РИА Новости [Электронный ресурс]. URL: https://ria.ru/20130524/939190083.html (дата обращения: 01.09.2023).
5. Где в России жить безопасно? Российская газета [Электронный ресурс]. URL: https://rg.ru/2004/11/19/atlas.html (дата обращения: 01.09.2023).
6. «Сибирские ученые оценивают опасность цунами на российских побережьях» – статья в газете «Наука в Сибири» [Электронный ресурс]. URL: https://icmmg.nsc.ru/ru/content/news/sibirskie-uchenye-ocenivayut-opasnost-cunami-na-rossiyskih-poberezhyah-statya-v-gazete (дата обращения: 01.09.2023).
7. Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21.12.1994 № 68-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_5295/ (дата обращения: 01.09.2023).
8. МЧС России. Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий [Электронный ресурс]. URL: https://mchs.gov.ru/ (дата обращения: 01.09.2023).
9. Постановление Правительства РФ от 30.12.2003 № 794 (ред. от 16.02.2023) «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» [Электронный ресурс]. 2003. URL:

https://www.consultant.ru/document/cons_doc_LAW_45914/492eda9f08b2b56e284a2ab0b4c8d3719f3a2585/ (дата обращения: 01.09.2023).

10. Песков Р.И. Основные используемые в МЧС России информационные системы // Интернет-журнал «Технологии техносферной безопасности». 2017. Т. 72, № 2. С. 1–24.

11. А.В. Вострых. Анализ информационных систем, используемых в МЧС России для мониторинга и прогнозирования чрезвычайных ситуаций. Сервис безопасности в России: опыт, проблемы, перспективы. Мониторинг, предотвращение и ликвидация чрезвычайных ситуаций природного и техногенного характера. 2021. С. 257–260.

12. А.П. Дроздов, Р.И. Песков. Проблемы информационного обеспечения в Единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций. Материалы II Международной заочной научно-практической конференции «Человеческое развитие: вызовы и перспективы» // «Human Progress». 2017. Т. 3, № 3. С. 1–24.

13. Ничепорчук В.В., Тасейко О.В. Мониторинг безопасности территорий. Сибирский государственный университет науки и технологий. Красноярск, 2023.

14. Государственный стандарт Российской Федерации. Мониторинг и прогнозирование. Термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200001516 (дата обращения: 01.09.2023).

15. Федеральный закон от 03.07.1998 «О гидрометеорологической службе» [Электронный ресурс]. 1998. URL: https://base.garant.ru/12112455/ (дата обращения: 04.08.2023).

16. Положение о государственной наблюдательной сети. РД 52.04.567-2003 [Электронный ресурс]. 2003. URL: https://docs.cntd.ru/document/1200034754 (дата обращения: 04.08.2023).

17. Федеральный закон от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности» (с изменениями и дополнениями) [Электронный ресурс]. URL: https://base.garant.ru/10103955/ (дата обращения: 01.09.2023).

18. Приказ Федерального агентства лесного хозяйства от 5 июля 2011 г. № 287 «Об утверждении классификации природной пожарной опасности лесов и классификации пожарной опасности в лесах в зависимости от условий

погоды» [Электронный ресурс]. URL: https://base.garant.ru/12189021/ (дата обращения: 01.09.2023).

19. Приказ Минсельхоза от 16 декабря 2008 г. № 13476 «Об утверждении классификации природной пожарной опасности лесов и классификации пожарной опасности в лесах по условиям погоды» [Электронный ресурс]. URL: https://rg.ru/documents/2009/03/18/klassifikaciya-dok.html (дата обращения: 01.09.2023).

20. Методические рекомендации по порядку работы с результатами оперативной аэрофотосъемки с целью мониторинга и прогнозирования чрезвычайных ситуаций. Москва. 2021 [Электронный ресурс].

21. С.В. Горбунов, С.А. Петелин. Система поддержки принятия управленческих решений в чрезвычайных ситуациях на основе прецедентного подхода // Стратегия гражданской защиты: проблемы и исследования. 2018. Т. 14, № 1. С. 74–87.

22. А.А. Рыженко и др. Системы поддержки принятия решений. Москва. 2016.

23. С.А. Качанов, С.Н. Нехорошев, А.П. Попов. Информатизационные технологии поддержки принятия решений в ЧС. Автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций: вчера, сегодня, завтра. Москва. 2011.

24. Н.Г. Топольский, В.Я. Вилисов. Методы, модели и алгоритмы в системах безопасности: машинное обучение, робототехника, страхование, риски, контроль; под ред. д-ра техн. наук, профессора Н.Г. Топольского. Москва. 2021.

25. Энциклопедия «Гражданская защита» под общей редакций С.К. Шойгу. 2006.

26. В.В. Ничепорчук, А.И. Ноженков, Л.Ф. Ноженкова. Программный комплекс ЭСПЛА-ПРО: средства сбора, аналитической обработки данных и поддержки принятия решений для органов управления МЧС России. СИББЕЗОПАСНОСТЬ-СПАССИБ. 2009. С. 114-123.

27. Н.В. Трофимова, О.А. Антамошкин, О.А. Антамошкина, В.В. Ничепорчук. Система поддержки принятия решений по реагированию на чрезвычайные ситуации и происшествия на опасных производственных объектах. Технологии гражданской безопасности. том 8, № 4 (30), 2011.

28. Федеральный закон «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» от 30.12.2015 № 431-ФЗ (последняя редакция). [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_191496/ (дата обращения: 01.09.2023).
29. Национальный стандарт Российской Федерации. Географические информационные системы. Термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200044680 (дата обращения: 01.09.2023).
30. ArcGIS Online. Cloud-based software to create and share interactive web maps [Электронный ресурс]. URL: https://www.arcgis.com/index.html (дата обращения: 01.09.2023).
31. ArcGIS Pro. Foundational user type for ArcGIS Online and ArcGIS Enterprise [Электронный ресурс]. URL: https://www.esri.com/en-us/arcgis/products/user-types/explore/gis-professional (дата обращения: 01.09.2023).
32. Самсонов Т.Е. Основы геоинформатики: практикум в ArcGIS [Электронный ресурс]. 2023. URL: https://tsamsonov.github.io/arcgis-course/ (дата обращения: 01.09.2023).
33. QGIS. Свободная географическая информационная система с открытым кодом [Электронный ресурс]. 2023. URL: https://www.qgis.org/ru/site/index.html (дата обращения: 01.09.2023).
34. Энтин А., Самсонов Т., Карпачевский А. Основы геоинформатики: практикум в QGIS [Электронный ресурс]. 2023. URL: https://aentin.github.io/qgis-course/ (дата обращения: 01.09.2023).
35. NextGIS – официальный сайт (ГИС) [Электронный ресурс]. 2023. URL: https://nextgis.ru/ (дата обращения: 01.09.2023).
36. Федеральный портал пространственных данных [Электронный ресурс]. 2023. URL: https://portal.fppd.cgkipd.ru/main (дата обращения: 01.09.2023).
37. Федеральная государственная информационная система территориального планирования [Электронный ресурс]. 2023. URL: https://fgistp.economy.gov.ru/ (дата обращения: 01.09.2023).
38. Геопортал Роскосмоса [Электронный ресурс]. 2023. URL: https://gptl.ru/ (дата обращения: 01.09.2023).

39. Информационная система дистанционного мониторинга Федерального агентства лесного хозяйства (ИСДМ-Рослесхоз). [Электронный ресурс]. 2023. URL: http://public.aviales.ru/main_pages/public.shtml (дата обращения: 01.09.2023).

40. Пожарная обстановка на особо охраняемых природных территориях федерального значения [Электронный ресурс]. 2023. URL: https://fires.minprirody.ru/ (дата обращения: 01.09.2023).

41. Геоинформационная система МЧС России «Космоплан» [Электронный ресурс]. URL: https://www.scanex.ru/thematic/projects/kosmoplan/ (дата обращения: 01.09.2023).

42. КГАУ «Лесопожарный центр». Карта лесных пожаров на территории красноярского края [Электронный ресурс]. 2023. URL: https://lpcentr.ru/index.php?option=com_content&view=article&id=100&Itemid=84 (дата обращения: 01.09.2023).

43. NASA FIRMS (Fire Information for Resource Management System) [Электронный ресурс]. 2023. URL: https://firms.modaps.eosdis.nasa.gov/map (дата обращения: 01.09.2023).

44. Global Forest Watch [Электронный ресурс]. 2023. URL: https://www.globalforestwatch.org/topics/fires/ (дата обращения: 01.09.2023).

45. NIFC Open Data Site. Federal interagency wildland fire maps and data for all [Электронный ресурс]. 2023. URL: https://data-nifc.opendata.arcgis.com/ (дата обращения: 01.09.2023).

46. Ahmadvand M., Pretschner A., Kelbert F. Chapter Eight - A Taxonomy of Software Integrity Protection Techniques / под ред. Memon A.M. Elsevier, 2019. Т. 112. С. 413–486.

47. Разведка через бэкдор: группировка Dark River штурмует российский оборонный комплекс [Электронный ресурс]. 2023. URL: https://www.securitylab.ru/news/542174.php (дата обращения: 01.09.2023).

48. Только не волчи: госорганизации атакует новая хакерская группировка [Электронный ресурс]. 2023. URL: https://iz.ru/1588238/ivan-chernousov/tolko-ne-volchi-gosorganizatcii-atakuet-novaia-khakerskaia-gruppirovka (дата обращения: 01.09.2023).

49. ФСТЭК Государственный реестр сертифицированных средств защиты информации [Электронный ресурс]. 2023. URL: https://reestr.fstec.ru/reg3 (дата обращения: 01.09.2023).
50. The immutable laws of security [Электронный ресурс] Microsoft. 2023. URL: https://learn.microsoft.com/en-us/security/zero-trust/ten-laws-of-security (дата обращения: 01.09.2023).
51. ФСТЭК Методический документ от 25 декабря 2022 г. Рекомендации по безопасной настройке операционных систем Linux [Электронный ресурс]. 2022. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-dekabrya-2022-g (дата обращения: 01.09.2023).

СПИСОК ИЛЛЮСТРАЦИЙ

СПИСОК СОКРАЩЕНИЙ

АИУС – Автоматизированная информационно-управляющая система РСЧС (АИУС РСЧС)

ВСМК – Всероссийская служба медицины катастроф

ГИМС – Государственная инспекция по Маломерным судам

ГИС – геоинформационная система

ГЗ – гражданская защита

ГО – гражданская оборона

ГосСОПКА – Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

ЕДДС – Единая дежурно-диспетчерская служба

ИС ПД (ИС ПДн) – информационная система персональных данных

КИИ – критическая информационная инфраструктура

НЦУКС – Национальны центр управления в кризисных ситуациях

НКЦКИ – Национальный координационный центр по компьютерным инцидентам

РСЧС – Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций

ЦУКС – центр управления в кризисных ситуациях

ЦОВ – центр обработки вызовов ЕДДС

ПО – программное обеспечение

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ФОИВ – федеральные органы исполнительной власти

ЧС – чрезвычайная ситуация

API – Application Programming Interface, программный интерфейс приложения

SOC – Security Operations Center, Центр мониторинга информационной безопасности

IDS/IPS – Intrusion Detection/Prevention System, Система обнаружения и предотвращения вторжений

IoT – Internet of Things, Интернет вещей

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЧС

учебное пособие

Авторы:

Матеров Евгений Николаевич – заведующий кафедрой физики, математики и информационных технологий Сибирской пожарно-спасательной академии ГПС МЧС России, кандидат физико-математических наук.

Бабёнышев Сергей Валерьевич – профессор кафедры физики, математики и информационных технологий Сибирской пожарно-спасательной академии ГПС МЧС России, кандидат физико-математических наук.