НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ОРГАНИЗАЦИИ
ЗДРАВООХРАНЕНИЯ И МЕДИЦИНСКОГО МЕНЕДЖМЕНТА
ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В ЗДРАВООХРАНЕНИИ ГОРОДА МОСКВЫ

НИИОЗММ:

МЫ РОЖДАЕМ СМЫСЛЫ.
СОЗДАЕМ ТОЧКИ РОСТА.
ФОРМИРУЕМ ТРЕНДЫ.
СТРОИМ БУДУЩЕЕ.
СОВЕРШЕНСТВУЕМ НАСТОЯЩЕЕ.
ДВИГАЕМ НАУКУ ВПЕРЕД!

ОГЛАВЛЕНИЕ

Елена Аксёнова

Директор Научно-исследовательского института организации здравоохранения и медицинского менеджмента Департамента здравоохранения города Москвы

«Юбилей – это важная веха в истории, становлении и прогрессе любой организации. Мы воспринимаем юбилей как двигатель развития, не останавливаемся на достигнутом, идем вперед. Наша задача – реагировать на самые смелые и неожиданные вызовы, проявлять инициативу, лидировать в исследовательских открытиях. Московское здравоохранение меняется столь стремительно и качественно, что все организации хотят соответствовать набранному темпу.

ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НИИ организации здравоохранения и медицинского менеджмента ДЗМ – оператор Департамента здравоохранения города Москвы по формированию контура информационной безопасности (ИБ) московского здравоохранения. Цифровой контур помогает обеспечить системный контроль за распространением информационных угроз в медицинских организациях города. ИБ-специалисты института создают новые уровни защиты от хакерских атак систем и данных, проводят тренировки, учат реагированию на компьютерные инциденты.

МЫ ДЕЛАЕМ ЗДРАВООХРАНЕНИЕ СИЛЬНЕЕ И СОЗДАЕМ ВОЗМОЖНОСТИ ДЛЯ УСПЕШНОГО РАЗВИТИЯ С ПОМОЩЬЮ ИТ-ТЕХНОЛОГИЙ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

- Информационная безопасность учреждений здравоохранения города Москвы
- Организация работы по правовой, организационной и инженерно-технической защите
- Предотвращение несанкционированного доступа к информационным системам
- Выявление и устранение возможных каналов утечки конфиденциальной информации
- Обеспечение безопасности оборудования и технических средств в учреждениях
- Обеспечение безопасности объектов критической информационной инфраструктуры
- Контроль за выполнением требований нормативных документов
- Организация расследований по фактам компьютерных инцидентов
- Разработка, ведение, обновление нормативных актов, регламентирующих порядок обеспечения информационной безопасности
- Организация и проведение обучения в области информационной безопасности
- Разработка и внедрение методических рекомендаций по информационной безопасности
- Организация безопасной работы в ЕМИАС и ЕГИСЗ

ЦЕННОСТИ

Для качественного обеспечения информационной безопасности в учреждениях здравоохранения города Москвы мы придерживаемся ценностей, которые выработаны годами.

ПОДДЕРЖКА

Поддержка в решении любых вопросов, связанных с безопасностью информации

ВНИМАТЕЛЬНОСТЬ

Точное изучение случаев любой сложности

ПРОФЕССИОНАЛИЗМ

Наш опыт и знания помогают пресечь утечку данных в учреждениях

КОМАНДНАЯ РАБОТА

Согласованные и сознательные действия, направленные на воплощение общей идеи

ДОВЕРИЕ

Своевременное получение качественной информации

ДОСТУПНОСТЬ

Эффективное и комфортное использование цифровых технологий, ресурсов и услуг

ИДЕОЛОГИЯ РАБОТЫ

- Защита данных медицинских организаций
- Методическая поддержка и консультирование по вопросам ИБ
- Постоянное совершенствование принципов работы медицинских организаций с информационными системами в едином цифровом контуре
- Переход на отечественное ПО
- Нормативно-правовое регулирование
- Особый подход к безопасности в организациях ДЗМ

НАДЕЖНОСТЬ И ПАРТНЕРСТВО

ГБУ «НИИОЗММ ДЗМ» – надежное экспертное учреждение системы столичного здравоохранения. Институт является центром компетенций по вопросам защиты информации во всех медицинских организациях, подведомственных Департаменту здравоохранения города Москвы. Центр ведет контроль, надзор, а также исследует, обучает и анализирует.

- За длительное время работы институт наладил связь с различными структурными подразделениями города Москвы (Департаментом информационных технологий города Москвы, Федеральной службой по техническому и экспертному контролю, Роскомнадзором и др.).
- Выстроил надежный план действий по реагированию на инциденты и выполнению задач по защите информации.
- Развитие долгосрочных и взаимовыгодных отношений с партнерами позволяет расширять спектр предоставляемых услуг, повышать качество обслуживания медицинских организаций и укреплять нашу репутацию на рынке.

СБЕР БАНК

INFOWATCH®

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭКОСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ДЗМ

В функции НИИОЗММ ДЗМ входит поддержка организаций ДЗМ

Правовая

- Разработка типовых нормативных документов.
- Обеспечение внутреннего контроля.
- Обучение работников учреждений по предотвращению информационных угроз.

Организационная

- Организация приема и обработки обращений субъектов ПДн.
- Обеспечение бесперебойной работоспособности сети.
- Мониторинг сетевого трафика.
- Обеспечение доступов для пользователей на рабочих местах.

Техническая

- Установка и контроль средств антивирусной защиты информации.
- Ограничение возможностей переноса информации.
- Настройка различного ПО.

Методическая

- Обучение по информационной безопасности.
- Онлайн-консультации и вебинары.
- Тренировки по реагированию на инциденты информационной безопасности.

ВСЕ ДАННЫЕ ЗДРАВООХРАНЕНИЯ
В БЕЗОПАСНОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРАХ

>65 000	работников обучены в области информационной безопасности
>100 000	работников обеспечены электронной подписью
>100	тренировок по реагированию на инциденты проведено
>78 000	пользователей подключены к ТДМ
>2000	инцидентов расследовано

249 УЧРЕЖДЕНИЙ,
подведомственных Департаменту здравоохранения города Москвы

ИЗ НИХ 54
крупных медицинских учреждения (больницы, медицинские центры), имеющие собственную масштабную ИТ-инфраструктуру

БОЛЕЕ 100 000 ПОЛЬЗОВАТЕЛЕЙ,
работающих в сети ДЗМ

Защищенная криптографическими средствами сеть передачи данных между Департаментом и учреждениями

ЦЕНТР КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- НИИОЗММ ДЗМ играет важную роль в обеспечении информационной безопасности всего столичного здравоохранения.
- Институт разрабатывает рекомендации для учреждений здравоохранения города Москвы в сфере нормативно-правового регулирования информационной безопасности, а также контроля и надзора за его исполнением.
- Институт взаимодействует с курирующими ведомствами, осуществляющими контрольно-надзорную деятельность по вопросам защиты информации, а также информирования об угрозах информационной безопасности, актуальных для инфраструктуры столичного здравоохранения.

МЕДИЦИНСКИМ УЧРЕЖДЕНИЯМ ГОРОДА МОСКВЫ МЫ МОЖЕМ ПРЕДЛОЖИТЬ:

- доступ в информационные ресурсы города Москвы;
- безопасность доступа и защиту информации;
- соответствие требованиям законодательства РФ;
- реализацию принятых решений по обеспечению информационной безопасности;
- сопровождение учреждений при проведении проверок и участие в реагировании на запросы контрольно-надзорных органов;
- организацию или проведение обучения работников по правилам ИБ и проверку знаний;
- настройку специализированного ПО;
- подготовку специалистов.

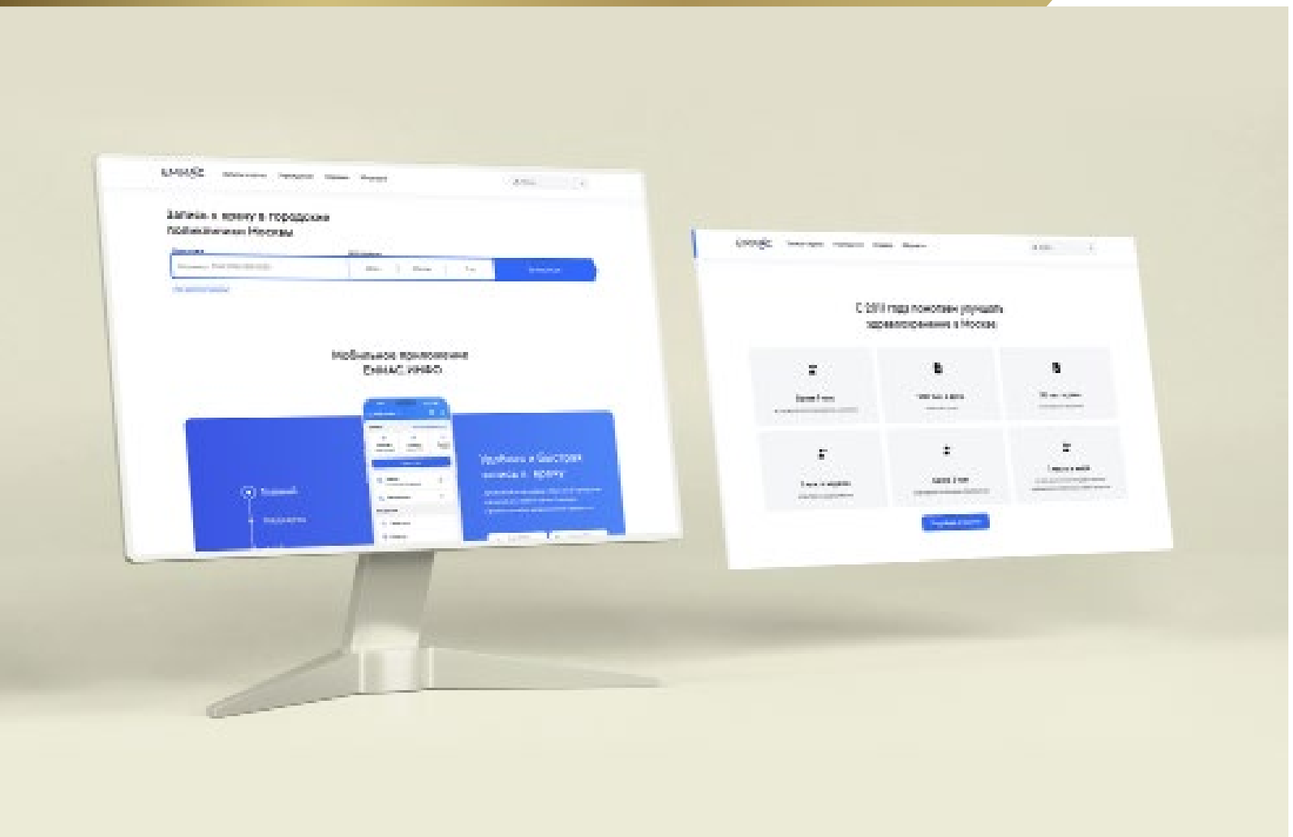
ПОДГОТОВКА РАБОТЫ В ЕГИСЗ

Информационное обеспечение в сфере здравоохранения осуществляется посредством создания, развития и эксплуатации федеральных государственных информационных систем в сфере здравоохранения, информационных систем в сфере здравоохранения Федерального фонда обязательного медицинского страхования и территориальных фондов обязательного медицинского страхования, государственных информационных систем в сфере здравоохранения субъектов Российской Федерации, медицинских информационных систем медицинских организаций, информационных систем фармацевтических организаций.

Мы предоставляем для учреждений здравоохранения:

- сопровождение защищенной сети передачи данных;
- техническую поддержку по вопросам работы в подсистемах ЕГИ;
- консультацию по вопросам получения доступа и настройки АРМ.

ПОДГОТОВКА РАБОТЫ В ЕМИАС



ЕМИАС (Единая медицинская информационно-аналитическая система) – это система, разработанная в Москве для повышения качества и доступности медицинской помощи в государственных учреждениях здравоохранения. Она включает электронную регистратуру, сервисы для сбора и систематизации историй болезней граждан, для выписки электронных рецептов.

Мы предоставляем для учреждений здравоохранения:

- управление доступом;
- ведение справочника должностей;
- защиту информации.

СМАРТ-КАРТЫ

Отдел ИБ НИИ организации здравоохранения и медицинского менеджмента также занимается согласованием выдачи смарт-карт медицинским работникам Департамента здравоохранения города Москвы.

Смарт-карта — индивидуальный идентификатор пользователя сети ЕМИАС (у каждого сотрудника, работающего в ЕМИАС, должна быть персонифицированная смарт-карта).

ПОДКЛЮЧЕНИЕ К БЕЗОПАСНОМУ МЕССЕНДЖЕРУ

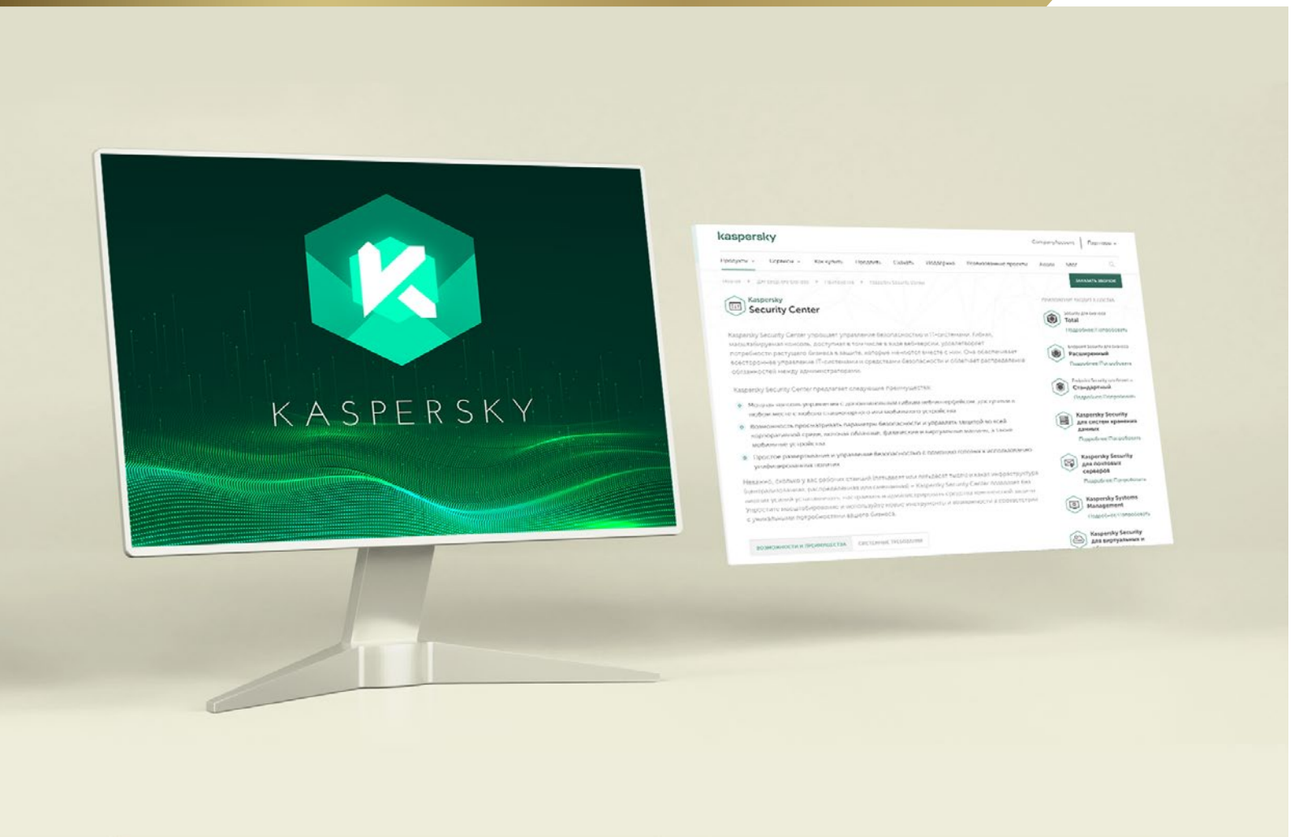
В **НИИОЗММ ДЗМ** подключают работников медицинских учреждений, а также сотрудников Департамента здравоохранения города Москвы к TDM.

Это электронный сервис «Мультисервисная коммуникационная платформа» с применением программного обеспечения клиентских программ мультисервисной коммуникационной платформы. TDM обеспечивает взаимодействие при исполнении трудовых функций работниками посредством голосовых вызовов и обмена мгновенными электронными сообщениями и документами с целью информационной безопасностии защиты данных внутри структуры учреждения.

TDM – это мессенджер для рабочей коммуникации, поэтому зарегистрироваться в нем могут только сотрудники организаций, подключенных в специальном порядке.

- Ежедневно подключаются новые пользователи
- Каждую неделю актуализируются телефоны (добавляются новые или удаляются из базы)
- Заявки на добавление или удаление телефонов направляются по форме непосредственно через мессенджер в ДИТ г. Москвы
- Также оказывается поддержка всем сотрудникам, направившим заявку с телефонами от учреждений
- Оперативно и своевременно добавляются номера телефонов для использования мессенджера первых лиц Департамента здравоохранения города Москвы

KASPERSKY SECURITY CENTER



Каждое государственное медицинское учреждение города Москвы входит в область нашей защиты. На рабочих станциях учреждения установлено антивирусное программное обеспечение, что значительно упрощает управление безопасностью и ИТ-системами поликлиник, стационаров, медицинских центров.

Благодаря данному ПО мы контролируем информационную безопасность, можем отследить место инцидента и эффективно и оперативно его устранить.

Полный обзор состояния защиты

Физические, виртуальные и облачные рабочие места управляются из единой консоли.

Оптимизация выполнения повседневных задач

Расширяемая архитектура консоли включает плагины для управления защитными продуктами для различных платформ.

ПРОФЕССИОНАЛЬНОЕ РАЗВИТИЕ ИТ-СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задачей Центра информационной безопасности является развитие профессиональных навыков и знаний специалистов по информационной безопасности.

Роль института для специалистов по информационной безопасности

- Обучение и развитие
- Подготовка квалифицированных кадров
- Обмен опытом и знаниями
- Консультирование и поддержка
- Анализ и исследования
- Участие в проектах и инициативах
- Сотрудничество с другими организациями

ОБУЧЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведение обучения в области информационной безопасности способствует повышению уровня грамотности работников учреждения, в том числе руководителей.

Это один из инструментов укрепления защиты данных и правильной безопасной работы с ними.

Чтобы работа с данными в учреждениях была безопасной, совместно с Департаментом информационных технологий города Москвы мы организовываем электронные курсы по основам информационной безопасности. Заявки на обучение принимаются каждый рабочий день.

Принято более 100 000 заявок на обучение

Более 20 000 работников успешно прошли курсы

Ежемесячно проводится анализ отчетов о прохождении обучения

ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

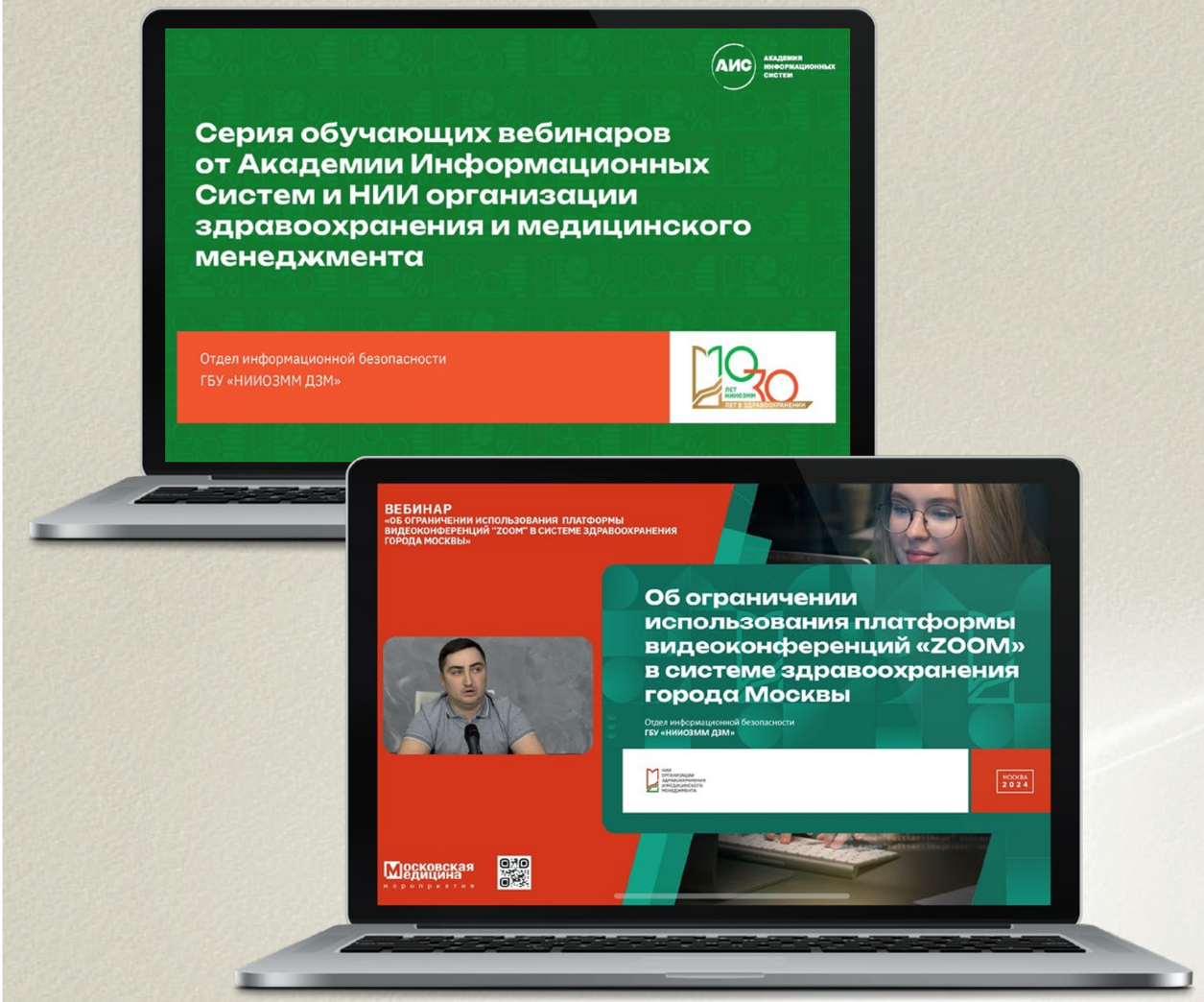
Центр информационной безопасности института разработал и внедрил в 2022 г. программу повышения квалификации по обеспечению безопасности объектов критической информационной инфраструктуры (КИИ) для специалистов в области информационных технологий и информационной безопасности.

Целью изучения программы повышения квалификации является совершенствование и(или) получение новых компетенций, необходимых для осуществления профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих) субъектов КИИ, ответственных за обеспечение безопасности объектов КИИ, функционирующих в сфере здравоохранения.

Более 1000 заявок

250 специалистов получили удостоверения о повышении квалификации

Обучающие программы, согласованные со **ФСТЭК России**



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В ЗДРАВООХРАНЕНИИ МОСКВЫ

Объекты критической информационной инфраструктуры – это информационные системы, сети, автоматизированные системы управления, телекоммуникационные и информационные ресурсы. Все они имеют очень важное значение в функционировании системы столичного здравоохранения и нуждаются в обеспечении безопасности, а также в построении системы защиты.

Нашей целью и задачей является координация подведомственных Департаменту здравоохранения города Москвы учреждений по вопросу обеспечения информационной безопасности объектов КИИ, предотвращение возможных угроз и реагирование на инциденты информационной безопасности.

- Методическое сопровождение и консультация по вопросам КИИ
- Формирование отчетов об объектах КИИ
- Анализ угроз

ПРОВЕДЕНИЕ ТРЕНИРОВОК ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

Согласно Комиссии по информационной безопасности при мэре города Москвы (КИБ Москвы), мы проводим показательные тренировки по реагированию на разные типы инцидентов ИБ на объектах КИИ в здравоохранении.

Основные цели

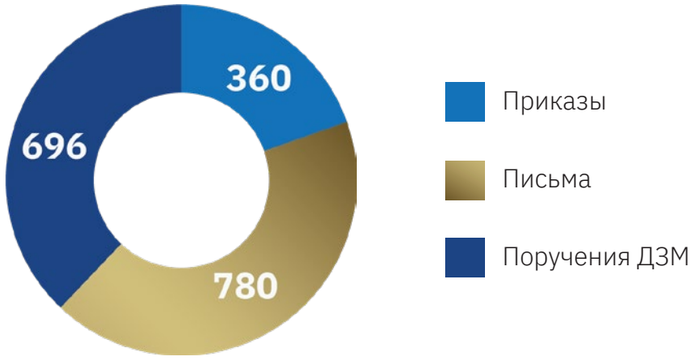
- Выявление слабых мест в инфраструктуре
- Оценка уровня защищенности объекта КИИ
- Усиление информационной безопасности учреждения
- Правильная настройка доступа
- Разъяснение законодательства РФ

Формат: очный.

Участники: медицинские организации ДЗМ.

НОРМАТИВНО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ РЕГУЛИРОВАНИЕ

Наш институт участвует в разработке и межведомственном согласовании федеральных законов, нормативных актов, рекомендательных писем и других документов по вопросам обеспечения информационной безопасности, киберустойчивости и применения информационных технологий в отношении учреждений здравоохранения. Эта работа ведется в том числе на основе анализа регуляторных и надзорных технологий с точки зрения рисков информационной безопасности. Также мы учитываем международный опыт по стандартизации и регулированию информационной безопасности.



- Приказы
- Письма
- Поручения ДЗМ

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

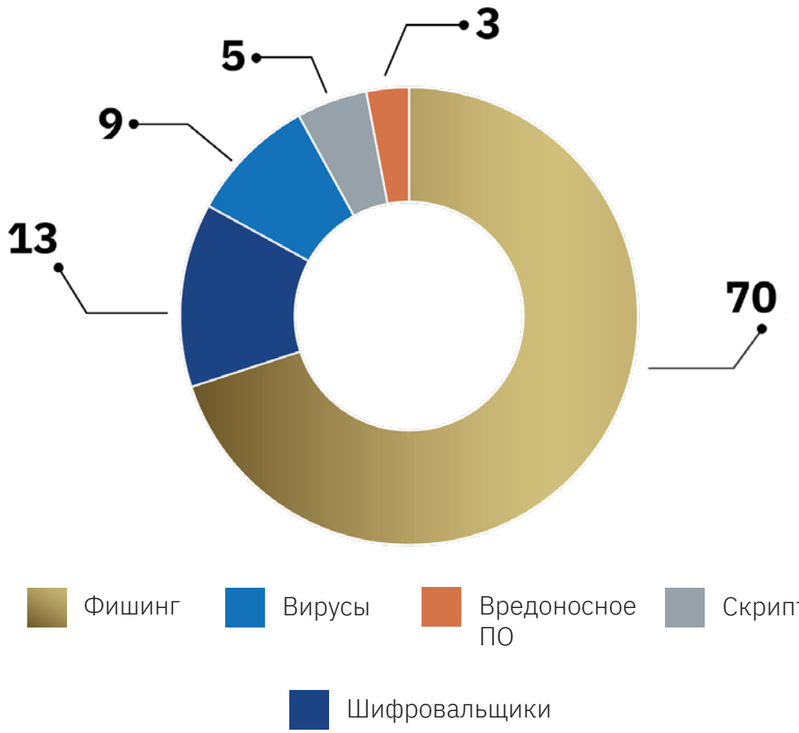
В нашем Центре информационной безопасности обрабатываются внешние запросы, поступающие из Национального координационного центра по компьютерным инцидентам, проверяются сайты на уязвимости и следы вторжения.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ОСНОВА УСТОЙЧИВОГО РАЗВИТИЯ

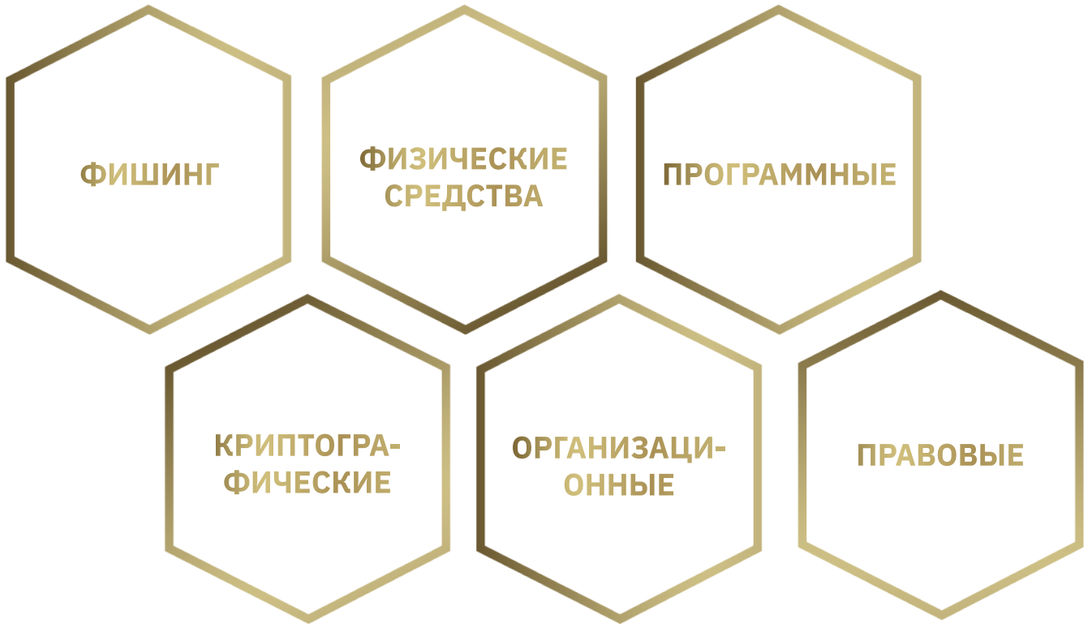
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ ДЗМ В 2023–2024гг.

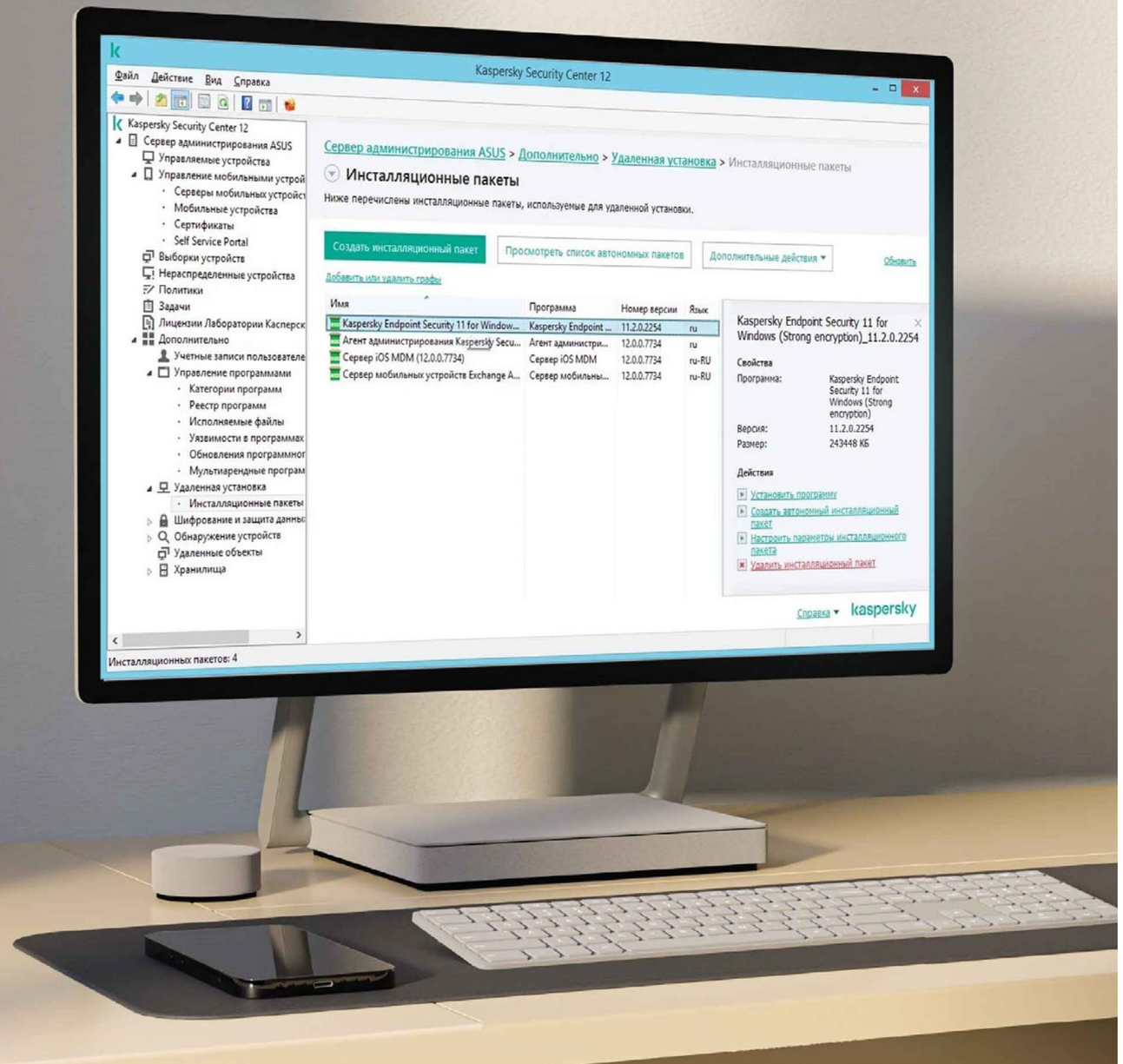
В 2023–2024 гг. возросло количество угроз информационной безопасности.

Мы регулярно проводим анализ сети, выявляем утечки информации, степень ущерба, источники угрозы.



ЗАЩИТА ИНФОРМАЦИИ. КОМПЛЕКС МЕР





МОНИТОРИНГ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ДЗМ

- Удаленная централизованная установка и удаление продуктов Лаборатории Касперского
- Удаленная централизованная настройка параметров продуктов
- Централизованное создание и удаленный запуск задач
- Управление лицензиями
- Автоматическое централизованное обновление антивирусных баз и модулей приложений
- Централизованный сбор и регистрация событий
- Централизованная рассылка уведомлений
- Создание сводных отчетов

Специалисты института ведут постоянный мониторинг работы сетей, отслеживают подозрительные действия на рабочих станциях

Также наши специалисты занимаются:

- базовой защитой от вирусов, троянских программ, червей, шпионских и рекламных программ
- проверкой файлов, почтовых сообщений, интернет-трафика
- мониторингом активности программ на компьютере
- защитой от программ-эксплойтов и программ блокировки экрана
- откатом действий вредоносной программы
- защитой от троянов-шифровальщиков
- проверкой Java и Visual Basic-скриптов
- защитой от скрытых битых ссылок
- постоянной проверкой файлов и защитой от фишинговых сайтов
- восстановлением корректных настроек системы после удаления вредоносного ПО
- созданием диска аварийного восстановления
- блокировкой ссылок на фишинговые сайты
- защитой от всех видов кейлоггеров
- автоматической настройкой программы
- технической поддержкой и автоматическим обновлением баз

ДЛЯ ЗАМЕТОК

НИИОЗММ –

ЭНЕРГИЯ
В ПАРТНЕРСТВЕ!


ЛЕТ
НИИОЗММ
ЛЕТ В ЗДРАВООХРАНЕНИИ