Информационная безопасность цифрового контура московской медицины

Сегодня без использования цифровых сервисов немыслимы ни лечебный процесс, ни научные исследования. Разветвленная цифровая сеть столичного здравоохранения относится к объектам критической информационной инфраструктуры и нуждается в надежной защите от хакерских атак и всевозможных сбоев.

Фото: mos.ruw

Защита медицинских организаций столицы

Для формирования контура информационной безопасности в московском здравоохранении в НИИ организации здравоохранения и медицинского менеджмента было создано управление информатизации. Это подразделение обеспечивает медицинским организациям города поддержку по любым вопросам, связанным с безопасностью информации. Институт является методологическим центром по вопросам информационной безопасности, имеет лицензию Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК) — государственного органа, выполняющего функции по координации и организации совместной работы ведомств в сфере госбезопасности по вопросам противодействия зарубежным техразведкам на территории РФ, защиты данных, относящихся к гостайне, отвечающего за безопасность важнейших точек информационной инфраструктуры РФ, а также занимающегося экспортным контролем.

Взаимодействие с Федеральной службой по техническому и экспортному контролю является неотъемлемой частью работы столичного здравоохранения по вопросам информационной безопасности.

В рамках взаимодействия организована работа по следующим направлениям:

1. Категорирование объектов критической информационной инфраструктуры.
2. Предъявление требований по технической защите информационных систем здравоохранения, а также соответствие этим требованиям.
3. Согласование программ профессиональной переподготовки и повышения квалификации.
4. Аттестация помещений и рабочих мест, в том числе и объектов информатизации.
5. Использование сертифицированных средств защиты информации.

В ведении специалистов по информационной безопасности сегодня находятся 249 учреждений, подведомственных Департаменту здравоохранения города Москвы:

- поликлиники,
- стационары,
- родильные дома,
- диспансеры,
- медицинские колледжи,
- санатории и др.

Из них 54 крупных медицинских учреждения (больницы, медицинские центры), имеющих свою собственную масштабную ИТ-инфраструктуру. В сети Департамента здравоохранения города Москвы насчитывается 60 серверов для обработки персональных данных работников и пациентов, постоянно находятся более 100 тысяч работающих пользователей.

В сети Департамента здравоохранения города Москвы насчитывается 60 серверов для обработки персональных данных работников и пациентов, постоянно находятся более 100 тысяч работающих пользователей.

ТРИ СОСТАВЛЯЮЩИЕ ПОДДЕРЖКИ УПРАВЛЕНИЯ ИНФОРМАТИЗАЦИИ НИИОЗММ, ОКАЗЫВАЕМОЙ МЕДИЦИНСКИМ ОРГАНИЗАЦИЯМ СТОЛИЦЫ ДЛЯ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ

ПРАВОВАЯ ПОДДЕРЖКА:
- разработка типовых нормативных документов;
- обеспечение внутреннего контроля;
- обучение работников учреждений предотвращению информационных угроз.

ОРГАНИЗАЦИОННАЯ ПОДДЕРЖКА:
- организация приема и обработки обращений медицинских организаций;
- обеспечение бесперебойной работоспособности сети;
- мониторинг сетевого трафика;
- обеспечение доступа для пользователей на рабочих местах.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ПОДДЕРЖКА:
- установка и контроль средств антивирусной защиты информации;
- ограничение возможностей переноса информации;
- настройка различного программного обеспечения.

Обучение по информационной безопасности

Центр информационной безопасности института разработал и внедрил программу повышения квалификации по обеспечению безопасности объектов критической информационной инфраструктуры для специалистов в области информационных технологий и информационной безопасности. Прохождение этого курса позволяет специалистам объектов критической информационной инфраструктуры сферы здравоохранения, ответственным за обеспечение их безопасности, повышать свой профессиональный уровень и получать новые компетенции. Обучение по этой программе прошли уже 100 специалистов, которые получили удостоверение о повышении квалификации.

Информационная безопасность объектов критической информационной инфраструктуры

Объекты критической информационной инфраструктуры — это информационные системы, сети, автоматизированные системы управления, телекоммуникационные и информационные ресурсы. Согласно Комиссии по информационной безопасности при мэре города Москвы, сотрудники управления информатизации проводят показательные тренировки по правильному реагированию на разные типы инцидентов информационной безопасности на объектах критической информационной инфраструктуры в здравоохранении. Уже проведено более 100 тренировок по реагированию на инциденты, регулярно формируются отчеты об этих объектах и анализируются угрозы для их безопасности.

Правовое регулирование

IT-специалисты НИИОЗММ подключают работников медицинских учреждений, а также сотрудников Департамента здравоохранения города Москвы к безопасному электронному мессенджеру TDM.

НИИОЗММ участвует в разработке и межведомственном согласовании федеральных законов, нормативных актов 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. В процессе работы также учитывается международный опыт.

Реагирование на компьютерные инциденты

В управлении информационной безопасности обрабатываются внешние запросы, поступающие из Национального координационного центра по компьютерным инцидентам, идет проверка сайтов на уязвимость и следы вторжения. На сотрудников управления возложена функция по мониторингу и реагированию на компьютерные инциденты, а также по ликвидации их последствий. За эти два года благодаря проведению тренировок по реагированию на инциденты в учреждениях здравоохранения они накопили значительный опыт в их анализе и устранении.

Современные решения по защите данных

Мониторинг антивирусного программного обеспечения медицинских организаций — это процесс автоматического отслеживания состояния информационной безопасности их сети. Благодаря мониторингу сети при помощи антивируса выявляется подозрительная активность, вторжения и другие угрозы безопасности, что позволяет оперативно реагировать и предотвращать атаки. Также мониторинг сети помогает оптимизировать работу сети и предотвращать перегрузки. ИТ-специалисты НИИОЗММ подключают работников медицинских учреждений, а также сотрудников Департамента здравоохранения города Москвы к электронному мессенджеру TDM — мультисервисной коммуникационной платформе для обеспечения взаимодействия сотрудников при выполнении рабочих задач посредством голосового вызова и обмена мгновенными электронными сообщениями и документами с целью информационной безопасности и защиты данных внутри структуры учреждения.