Возможно ли защитить персональные данные в Телемедицине? | **13**

ИТ

Тематическое приложение к газете **Коммерсантъ**

Информационные технологии

Четверг 25 апреля 2019 №74 (6554 с момента возобновления издания)

ufa.kommersant.ru

13 | Перейдет ли ЖКХ в цифру?

15 | Когда в Башкирию придут мобильные сети пятого поколения?

Телемедицине не хватает защиты

С момента принятия закона о телемедицине в Башкирии к Единой государственной системе в сфере здравоохранения (ЕГСИЗ, — прим. «ИТ») подключились все государственные медицинские учреждения. Принятые Курултаем РБ поправки позволяют вести онлайн-приемы и частным клиникам. Однако все еще открытым остается вопрос защиты персональных данных. Недостаточное внимание к вопросам информационной безопасности в этой сфере может привести, в том числе, к утечкам в сеть историй болезней, или получению злоумышленниками контроля над медицинской аппаратурой.

— киберзащита —

ДМИТРИЙ ЛЕБЕДЕВ

После запуска телемедицины в регионе стал актуальным вопрос защиты данных пациентов

Закон о телемедицине в России вступил в силу 1 января 2018 года. После его принятия врачи могут давать онлайн-консультации и вести наблюдение за здоровьем пациента удаленно. Телемедицину в Башкирии развивают в рамках федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации» и федерального проекта «Цифровой контур здравоохранения» национальной программы «Здравоохранение».

Для того, чтобы начать работу в этом направлении, республиканским больницам нужно было зарегистрироваться в реестре медицинских организаций ЕГСИЗ, а врачам — в Федеральном регистре медицинских работников, предусмотрено было также подключение к Центру дистанционных консультаций (ЦДК, — прим. «ИТ»). В настоящий момент к системе подключены все медицинские организации республики трех уровней.

В 2018 году в Госсобрании — Курултае РБ были приняты поправки в закон «О частной медицинской деятельности в Республике Башкортостан» от 2002 года, после чего телемедицина стала также доступна и для частных республиканских клиник. Частным медикам в Башкирии разрешено выписывать электронные назначения, выдавать справки-файлы, рецепты на лекарства, вести консультации. При принятии законопроекта отмечалось, что переход в коммерческих клиниках на цифровую документацию не требовал дополнительного финансирования, так как материальная база была полностью готова.

В 2018 году в регионе больше всего телеконсультаций прошло в Республиканском кардиологическом центре — 803, в Республиканском клиническом перинатальном центре — 763, в Республиканской клинической больнице имени Куватова — 579. Активной также была Учалинская больница, городская клиническая больница №13 в Уфе, городская больница в Кумертау.

Всего в 2018 году медицинскими организациями республики проведено свыше 3,7 тысячи телеконсультаций, из них 225 — с федеральными центрами. В 2017 году состоялась 3031 медицинская консультация онлайн. Большая доля приемов онлайн была связана с вопросами кардиологии, онкологии, сосудистой хирургии — 54% от общего числа.

Новые угрозы

Одной из самых серьезных проблем развития сферы телемедицинских услуг эксперты называют защиту персональных данных. Недостаточная оснащенность оборудованием, отсутствие законодательного регулирования и компетентных сотрудников в кибербезопасности могут привести, как минимум, к разглашению истории болезни пациентов.

Регулирование деятельности по обработке и использованию персональных данных в России определяется ФЗ-152 «О персональных данных». За безопасность персональных данных отвечает оператор системы: организации, которые хранят, собирают, передают или обрабатывают персональные данные, должны выполнить ряд технических и организационных требований по защите этой информации. Каждая организация обязана иметь пакет документов, подтверждающий защищенность персональных данных.

Однако стандартных мер защиты персональных данных для телемедицины недостаточно.

«В телемедицине оператор может наткнуться на некоторые «подводные камни», с которыми он не сталкивается при обработке персональных данных в других информационных системах. Это связано с тем, что в телемедицине обрабатываются специальные категории и биометрические данные о состоянии здоровья пациента, физиологические и биологические особенности человека. Такие данные требуют принятия дополнительных мер защиты», — поясняет директор филиала АО «ЭР-Телеком Холдинг» (ТМ «Дом.ru Бизнес», «Дом.ru») в Уфе Ольга Карелина. с14

ЖКХ перейдет на цифру

— тенденции —

Регистрация всех участников жилищно-коммунального хозяйства Башкирии в федеральной государственной системе ЖКХ открыла перспективы для развития цифрового рынка в сфере коммунальных услуг. Экономическую выгоду видят и бизнес, и государство, и конечный потребитель. Осталось определить, кто должен нести затраты на внедрение новых технологий. Тем не менее, заявления о готовности реализовывать «умные» технологии в ЖКХ Башкирии уже сделали крупные российские телеком-игроки.

Цифровизация ЖКХ в России и, в частности, в Башкирии началась с обязательной регистрации участников рынка жилищно-коммунальных услуг в государственной информационной системе ЖКХ (ГИС ЖКХ, — прим. «ИТ»). Согласно закону «О государственной информационной системе жилищно-коммунального хозяйства» (№ 209 ФЗ), коммунальные службы и поставщики энергии должны быть зарегистрированы в этой системе и регулярно отчитываться перед потребителями. С 1 января 2018 года нарушение сроков и порядка размещения информации в системе, либо ее размещение не в полном объеме, либо заведомо ложной информации влечет за собой административную ответственность в виде штрафа для должностных лиц в размере 30 тыс. руб., для юридических лиц — 200 тыс. руб.

В федеральной информационной системе ГИС ЖКХ собрана вся информация о состоянии жилищного фонда, стоимости коммунальных услуг, задолженностях, работах по содержанию и ремонту общего имущества в многоквартирных домах. Как сообщается на сайте республиканского министерства жилищно-коммунального хозяйства, в регионе в системе зарегистрировано 100% компаний, предоставляющих услуги ЖКХ. Всего по данным сайта ГИС ЖКХ, в Башкирии зарегистрировано 1810 организаций, более 49,6 тыс. многоквартирных и около 407, 9 тыс. жилых домов. Как пояснил замминистра жилищно-коммунального хозяйства Башкирии Марат Шангареев, внедрение ГИС ЖКХ сделает сферу жилищно-коммунального хозяйства более прозрачной и даст возможность гражданам получать актуальную информацию об управляющих и ресурсоснабжающих организациях, о выполняемых работах по дому и доступных услугах.

«Российские города, на мой взгляд, находятся в начале большого пути по цифровизации коммунальной сферы. В регионе активнее всего на рынке IoT (англ. Internet of Things — интернет вещей, — прим. «ИТ») в коммунальной сфере работают «Башинформсвязь» и «Эр-Телеком». В августе прошлого года в Уфе запущены беспроводная радиосеть на базе технологии связи LoRaWAN (англ. Low-power Wide-area Network — энергоэффективная сеть дальнего радиуса действия, — прим. «ИТ») и решение, предназначенное для удаленного сбора данных с приборов учета, в том числе и общедомовых, в режиме реального времени. Нельзя сказать, что Башкирия находится в авангарде по темпам развития цифровой сети ЖКХ, но мы точно не в хвосте», — сообщил руководитель направления инфраструктурных решений Softline в ПФО Олег Садыков.

Цифруют все

С развитием технологий у отрасли ЖКХ расширяются возможности. Для телеком-операторов и разработчиков цифровые решения в жилищно-коммунальном хозяйстве (ЖКХ, — прим. «ИТ») — новый перспективный рынок. Цифровые решения в области ЖКХ — компонент реализации «Умного города», концепция которого появилась в рамках государственной программы «Цифровая экономика». В основном, все цифровые сервисы «Умного города» планируется применять в энергоснабжении и теплосетях.

«Конечно, в такой ситуации бизнесу эта тема становится интересной. Госкорпорации не работают на «глухих» рынках, и частный бизнес это понимает. Власть и города заинтересованы в цифровизации ЖКХ. Отрасль традиционно вызывает много негатива, в том числе за счет «непрозрачности» процессов. Повышение прозрачности приводит к росту конкуренции на рынке услуг управляющих компаний, а соответственно и к снижению социальной напряженности», — рассказал представитель ГК «Исерв» Максим Иванов.

Важным этапом в цифровизации ЖКХ станет автоматическое снятие и передача данных со счетчиков в ЖЭУ и управляющие компании. В каждом счетчике будет стоять специальная электронная головка с передачей показаний в режиме онлайн. Минстроем РФ предложен законопроект, который сделает установку дистанционных приборов учета обязательной. с16

НЕОБХОДИМОСТЬ КИБЕРЗАЩИТЫ МАЛОГО И СРЕДНЕГО БИЗНЕСА: МИФ ИЛИ РЕАЛЬНОСТЬ?

Зачастую собственники и руководители среднего и малого бизнеса не уделяют должного внимания информационной безопасности, полагая, что киберпреступников могут заинтересовать только крупные корпорации. Но опыт показывает, что это не так. Данный сегмент бизнеса не менее привлекателен для мошенников: вероятность успешной атаки на небольшие компании заметно выше из-за большого количества уязвимостей в системах информационной безопасности. Зачастую представители среднего и малого бизнеса сами по себе не являются целью, но могут быть использованы в качестве плацдарма для целевой атаки на корпорации из-за недоработок в цифровой защите.

По данным исследований американской телеком-компании Verizon, около 30% инцидентов в сфере кибербезопасности приходится на компании со штатом не более 100 человек. Как минимум в одном из десяти случаев атаки хакеров приводят к утечке конфиденциальных данных, разглашение которых способно нанести серьезный урон бизнесу или репутации предприятия. Возмещение ущерба и устранение последствий может серьезно ударить по бюджету небольшой компании.

По прогнозам компании ESET, разработчика антивирусного ПО, в 2019 году произойдет дальнейшее усложнение киберугроз и разработка новых векторов атак. Рост числа киберпреступлений делает вопросы информационной защиты особенно актуальными для компаний малого и среднего бизнеса. Каждой организации для предотвращения утечки ценной информации и минимизации риска столкновения с угрозами стоит использовать комплексные защитные решения. Наряду с внедрением современных аппаратных и программных решений для безопасности важно повышать информационную грамотность персонала. В этом помогут консалтинговые услуги в области кибер-защиты (социотехнические тесты, веб-аудит, пентесты и др.), регулярное обучение сотрудников.

Для защиты цифровой инфраструктуры организаций подходят современные решения от федерального телеком-оператора «Дом.ru Бизнес», которые корпоративные клиенты могут выбрать на сайте www.b2b.domru.ru или по телефону 8 800 222 08 13. Обеспечить непрерывную работу бизнеса, защитив сайт от взлома и похищения конфиденциальных данных поможет профессиональная защита от DDoS-атак. Облачный сервис быстро распознает все известные виды атак, защищает сервер и эффективно отражает атаки, минимизируя тем самым последствия, финансовые и репутационные риски.

«Антивирусы для бизнеса» обеспечат офисный контроль и контроль устройств, надежную защиту от вредоносного ПО, спама и хакерских атак на сервера, ПК, мобильные устройства и локальные сети. Использование лицензионных антивирусов по подписке (Dr.Web, ESET, Kaspersky) позволяет корпоративным клиентам упростить администрирование и снизить расходы на информационную безопасность предприятия.

Также клиенты могут воспользоваться сервисом контент-фильтрации без дополнительного программного обеспечения и оборудования. Решение призвано выполнить требования законодательства по защите пользователей от нежелательной информации, такой как экстремистские сайты и прочих ресурсов, подлежащих ограничению. Это особенно актуально для учебных заведений и госучреждений.

«Федеральный телеком-оператор «Дом.ru Бизнес» предоставляет корпоративным клиентам не только надежные каналы передачи данных и облачные продукты. Ориентируясь на тенденции и потребности рынка, мы предлагаем решения по защите сетевой инфраструктуры и информации от киберугроз. При этом клиентам удобно использовать комплексное решение от одного оператора, подобрав его в зависимости от масштаба компании», – комментирует Ольга Карелина, директор филиала АО «ЭР-Телеком Холдинг» (ТМ «Дом.ru Бизнес», «Дом.ru») в Уфе.

информационные технологии

Телемедицине не хватает защиты

с13

Медицинские организации, использующие компоненты телемедицины, обязаны обеспечить защиту системы от несанкционированного доступа и вирусных атак, а также защиту каналов передачи данных, внедрить решения для обнаружения вторжений и анализа надежности. Для идентификации пациентов должна использоваться единая система идентификации и аутентификации на Госуслугах, документирование информации об оказании медицинской помощи пациенту с применением телемедицинских технологий должно осуществляться с использованием усиленной квалифицированной электронной подписи, сообщает директор «ИТ Энигма Уфа» Александр Оводов и в то же время отмечает, что в защите есть пробелы.

«Телемедицина — это стремительно развивающийся рынок, на него выходит большое количество компаний и сервисов. Разрабатываются такие сервисы и приложения в большинстве своем без учета требований к обеспечению информационной безопасности. В результате разработанное программное обеспечение, приложения для мобильных устройств имеют уязвимости, которыми пользуются злоумышленники. Кроме того, многие компании, эксплуатирующие телемедицинские сервисы, не знают о требованиях информационной безопасности или частично их игнорируют. В результате становятся легкой мишенью злоумышленников, которые незаконно получают персональные данные пациентов и продают их на черном рынке или используют против пациентов. Яркие свежие примеры недостаточной защищенности персональных данных пациентов — базы данных двух крупных телемедицинских сервисов оказались в открытом доступе. Кроме того, при передаче организации обязаны использовать сертифицированные ФСБ средства криптографической защиты информации. Еще несколько лет назад на рынке не было сертифицированных решений, которые бы могли обеспечивать безопасность передачи данных между врачами и пациентами без покупки пациентами средств криптографической защиты информации. Сейчас такие решения есть, но используют их единицы», — отмечает он.

Иван Працкевич, специалист компании Mindray-shop.ru, занимающейся поставкой интеграций и разработкой системных решений для медицины отмечает, что помимо утечек данных пациентов, злоумышленники могут получить контроль и над медицинским оборудованием. «Пример — больница из небольшого города республики хочет показать федеральному центру данные своего пациента. Допустим, чудо — и в ЦРБ есть DICOM (Digital Imaging and Communications in Medicine — медицинский отраслевой стандарт создания, хранения, передачи и визуализации цифровых медицинских изображений и документов обследованных пациентов, — прим. «ИТ»), и мы можем отправить снимки КТ, рентген, МРТ, УЗИ-исследования. Может, даже настроена LIS (Laboratory information system — лабораторно-информационная система, прим. «ИТ»), и тогда есть доступ к анализам, которые были сделаны или назначены. Но в 99% случаев консультация ограничится письмом по электронной почте. В удаленных районах республики, для которых телемедицина необходима в первую очередь, отсутствуют элементарно специалисты, способные работать на современном оборудовании. После запуска всего этого механизма в массовом порядке, безусловно, необходим специальный канал передачи информации. Так как в противном случае, используя сеть WI-FI для посетителей, можно получить доступ не только в раздел с персональными данными, LIS-диагнозами и назначениями, но и взаимодействовать с критически важными системами наркозно-дыхательной аппаратуры, инфузионными системами, техникой для искусственного кровообращения и т.п. На сегодня наши клиники не готовы к подобному типу угроз полностью».

ОЛЕГ ХАРСЕЕВ

В условиях законодательных пробелов следить за защитой персональных данных должны прежде всего сами клиники

Рассчитывать на собственные силы

Опрошенные «ИТ» эксперты отмечают, что для развития защиты персональных данных в телемедицине необходимо принять соответствующие законодательные акты — действующих недостаточно.

В Роскомнадзоре планируют рассмотреть вопрос нормативного установления заданных параметров качества связи в сегментах, связанных с обеспечением жизни и здоровья человека. Начальник Управления контроля и надзора в сфере связи Роскомнадзора Денис Пальцин отметил, что вопросы качества оказываемых в Российской Федерации услуг связи, в медицинской среде нормативно-правовыми актами не урегулированы, поскольку были выведены из-под регулирования и отданы конкурентному рынку в период конца 80-х — начала 90-х годов.

Однако вопрос совершенствования нормативной базы может оказаться намного шире одной только сферы телемедицины. По мнению руководителя отдела Департамента информационной безопасности ООО «Сервионика» Александра Сальникова, удаленный мониторинг здоровья с использованием медицинских приборов соответствует парадигме «Интернета вещей», для которого российских стандартов пока нет. «На сегодня, пожалуй, единственным прикладным отраслевым документом в области защиты информации в медицине, не считая общеизвестных и частично устаревших ГОСТов, являются «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» от 2009 года. Их явно недостаточно с учетом современного развития информационных технологий. Отстают от современных ИТ-реалий и нормы регулирования в области телемедицины: отраслевого стандарта по информационной безопасности для этой сферы пока нет», — считает он.

В ситуации законодательных пробелов, следить за сохранностью информации должны, прежде всего, сами клиники. Юрист Александр Болдырев отмечает, что каждое медицинское учреждение должно иметь серьезный набор внутренних нормативных документов и средств защиты информации на случай хранения, обработки и передачи персональных данных пациентов. Должен быть назначен сотрудник, непосредственно и лично отвечающий за их сохранность, считает он.

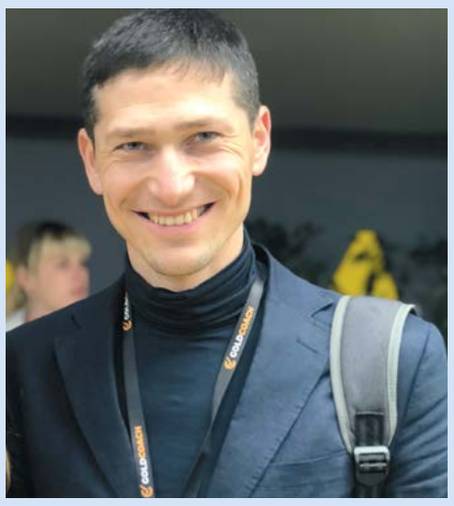
«Кибербезопасность обеспечить не очень сложно. Есть области, где комплекс мер по соблюдению безопасности опережает медицину, например, банковская сфера. И опыт отраслей-передовиков может быть применим и к здравоохранению. Есть прямая корреляция между применяемым комплексом мер по защите персональной информации, ценностью этих данных и возможными негативными последствиями для субъектов персональных данных, если они попадут к злоумышленникам. В России ценность персональных медицинских данных не очень высока по сравнению с другими развитыми странами. И возможные негативные последствия в России сравнительно ниже. Например, в ряде стран стоимость медицинского полиса напрямую зависит от состояния здоровья пациента, и утечка персональных медицинских данных может существенно сказаться на стоимости полиса. Например, наличие онкологического заболевания может быть косвенно причиной в отказе приема на работу. Сейчас мы проходим этап осознания ценности персональных медицинских данных и оценки возможных рисков в случае их утечки. Осознавая возможные последствия, мы предъявляем все более жесткие требования к защите личной информации, совершенствуем законодательную базу», — подчеркивает глава отдела цифрового здравоохранения компании Philips в России и СНГ Сергей Лаванов.

Лида Богатырева

ЦИФРОВАЯ МЕДИЦИНА

Как обеспечить безопасность данных пациентов

При строительстве, модернизации и эксплуатации медицинских объектов, телемедицинских сервисов важно учитывать необходимость обеспечения информационной безопасности. Директор компании «ИТ Энигма Уфа» Александр Оводов рассказал о требованиях к системам безопасности в медицинской отрасли, чем грозит отсутствие их соблюдения, и почему важно об этом задумываться еще на этапе составления бизнес-плана и проектирования.



— Сейчас медицинская отрасль не такая, как раньше. Почему, на ваш взгляд, так важна информатизация в этой сфере?

— Понятно, что современная медицина немыслима без использования информационных технологий — это и медицинские информационные системы, цифровое лабораторное оборудование, компьютерная томография, аппараты УЗИ, средства мониторинга состояния пациента, медицинское оборудование, используемое при проведении медицинских вмешательств, средства и сервисы дистанционного консультирования пациентов и даже 3D-принтеры. Построенные и проектируемые сейчас современные клиники уже оборудуются цифровыми автоматизированными системами жизнеобеспечения и мониторинга состояния пациентов; системами вентиляции, кондиционирования, управления освещением, температурой в помещениях. Все указанные информационные системы, автоматизированные системы управления и объединяющие их сети являются объектами информационной инфраструктуры организации.

— Расскажите, пожалуйста, как регулируется кибербезопасность в медицине?

— Помимо обеспечения безопасности персональных данных (152-ФЗ) появилась необходимость обеспечивать защиту информационной инфраструктуры. Она должна осуществляться в соответствии с 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконными актами. К сожалению, на практике, медицинские организации не знают всего объема требований по информационной безопасности, которые им необходимо выполнить, не говоря уже о их реализации. Если взять 152-ФЗ, то «за кадром» часто остаются Постановление Правительства №1119, Приказ ФСТЭК №21, Приказ ФСБ №378. Для 187-ФЗ — это Постановление Правительства №127, Приказы ФСТЭК 229, 235, 236, 239, Приказы ФСБ 366, 367, 368.

— Чем грозит их невыполнение?

— Невыполнение требований может привести не только к административной ответственности и штрафам, уже измеряющимися сотнями тысяч рублей, но и к уголовной. В частности, одновременно с 187-ФЗ были внесены изменения в Уголовный Кодекс Российской Федерации и введена уголовная ответственность на срок до шести лет лишения свободы при нарушении правил эксплуатации и правил доступа к персональным данным пациентам, если оно повлекло причинение вреда, и на срок до 10 лет при тяжких последствиях.

— Что произойдет если не учесть требования информационной безопасности на этапе проектирования?

— Во-первых, затраты на построение системы защиты информации, ее эксплуатацию, не будут заложены в финансовую модель. Как следствие расчеты рентабельности, срок возврата инвестиций, срок выхода на точку безубыточности будут определены некорректно. Во-вторых, может потребоваться изменение топологии локальной сети, и, как следствие, проведение дополнительных строительных работ. В-третьих, могут потребоваться дополнительные серверные и телекоммуникационные шкафы под размещение программно-аппаратных комплексов средств защиты информации, источников бесперебойного питания. В-четвертых, может потребоваться увеличение или изменения конфигурации серверов и рабочих мест пользователей.

— Как можно избежать этих затрат?

— Избыточных затрат можно избежать, если проектировать систему защиты информации одновременно с выбором информационных систем, медицинского оборудования, автоматизированных систем управления.

— А что делать, если медицинская клиника уже функционирует?

— Для действующих медицинских организаций необходимо в срок до 1 сентября 2019 года провести работы по определению объектов информационных инфраструктур, подлежащих категорированию в соответствии с 187-ФЗ, затем направить их перечень во ФСТЭК России. Дальше уже проводить категорирование объектов, проектировать и строить систему защиты.

— Какие есть особенности при онлайн-взаимодействии медицинской организации с клиентами?

— Если организация выходит в онлайн взаимодействие с клиентом, то особое внимание следует уделить защите сайта и мобильного приложения. Необходимо применять специализированные межсетевые экраны для веб-приложений, осуществлять анализ исходного кода приложений на отсутствие уязвимостей, озаботиться внедрением отечественных средств криптографической защиты информации в приложения и сайты для защиты передаваемых данных, периодические проводить анализ защищенности. Если этого не делать, доступ к персональным данным может оказаться в открытом доступе, как например, это произошло в марте с телемедицинским сервисом DOC+ и в апреле с CMD.

— Как быть организациям, которые оказывают телемедицинские услуги?

— На них распространяются те же требования, что и на медицинские организации, которые выходят на онлайн-взаимодействие с клиентами.

— Может ли в этом помочь ваша компания?

— Да, можем. На этапе разработки инвестиционных проектов можем провести оценку исходных данных и сделать расчет стоимости системы защиты. На этапе проектирования, как лицензиаты ФСТЭК и ФСБ, готовы осуществить разработку проектных решений на систему защиты. На этапе ввода в эксплуатацию и для работающих клиник осуществить внедрение средств защиты информации, разработку организационно-распорядительных документов, провести анализ защищенности всей информационной инфраструктуры.

На этапе эксплуатации взять на себя все заботы обеспечения информационной безопасности — от сопровождения средств защиты информации до взаимодействия с регуляторами (Роскомнадзором, ФСТЭК, ФСБ). Для онлайн-сервисов осуществляем приемку исходного кода приложений на соответствие требованиям информационной безопасности (поиск уязвимостей в коде).

РЕКЛАМА

Пятый элемент

— стратегия —

Телекоммуникационная отрасль стоит на пороге внедрения нового поколения мобильной связи. Ожидаемые технологические инновации стандарта 5G увеличат пропускную способность сетей мобильных операторов и скорость передачи данных. Крупные операторы в Башкирии уже начали запуск и тестирование сетей на больших скоростях. Однако активно развиваться новому стандарту мешает отсутствие свободных частот и высокая стоимость строительства сетей.

ОЛЕГ ХАРСЕЕВ

В Башкирии готовятся к запуску сетей пятого поколения

Раскинуть сети

По данным исследования аудиторской компании PWC, первые релизы спецификаций сети пятого поколения в мире были выпущены в декабре 2017 года. Завершить работу по развертыванию 5G планируется в период со второй половины 2018 до конца 2019 года.

Анонсируемые технологии пятого поколения мобильный связи — 5G обещают кардинально изменить представления о передаче данных. Заявлена максимальная скорость передачи данных до 20 Гбит/с, сверхнизкая задержка передачи данных — менее 1 мс, поддержка большого количества абонентских устройств — до 1 млн на 1 кв. км, расширенная поддержка специализированных сервисов, задействование нового радиочастотного спектра, включая миллиметровые волны. Согласно аналитике компании Ericsson, к 2023 году в сетях связи 5G будет зарегистрирован 1 млрд подключений. Услуги на базе пятого поколения к этому времени будут доступны для 20% мирового населения.

«Пятое поколение мобильной связи открывает огромные возможности для развития интернета вещей, сервисных услуг, безопасности в городском масштабе. Одно из основных требований к 5G — возможность передачи данных со скоростью в десятки мегабит в секунду для десятков тысяч пользователей одновременно. Это откроет возможности для глобального роста видеонаблюдения в целом: увеличится число мобильных клиентов, увеличится число камер и, как следствие всего этого, вырастет и уровень безопасности на конкретных объектах, в городах, странах. Если резюмировать, 5G открывает множество коммерческих выгод для тех, кто работает с интернетом вещей», — рассказывает технический директор компании-разработчика программного обеспечения для интеллектуального наблюдения «Сателлит Инновация» Виталий Тепляшин.

В России внедрение 5G осуществляется согласно госпрограмме «Цифровая экономика». Запланировано, что к 2020 году сети пятого поколения должны заработать в восьми городах России. К настоящему моменту тестовые зоны 5G реализованы у крупных телеком-операторов. Технологию тестировали в городах-организаторах чемпионата мира по футболу, А также на территории Сколково. У «Ростелекома» зона 5G расположена в Эрмитаже, а «Мегафон» летом 2018 года запустил ее в центре Москвы. Tele2 уже несколько лет тестирует сценарии применения 5G в разных отраслях промышленности. Строительство инфраструктуры в городах начнется после согласования использования частот на уровне регуляторов.

Операторы Башкирии готовятся к запуску пятого поколения, развивая инфраструктуру, но пока это сети 4G, на базе которых можно будет в дальнейшем развернуть 5G. В частности, для этих целей компания МТС совместно с Ericsson и Qualcomm выбрали Уфу. Запуск и тестирование высокоскоростной LTE-сети гигабитного класса с поддержкой технологии LAA. состоялся в ТРЦ «Планета». Инфраструктура «МегаФона» в регионе к развертыванию готова — однородная сеть позволяет быстрее внедрять технологии для ускорения мобильного интернета 4G, а в перспективе для развертывания 5G. Региональный оператор «Башинформсвязь» получил долю 50% в московском ООО «Диджитал для бизнеса». Компания является совместным предприятием «Ростелекома» и «МегаФона», созданным для развития сетей 5G.

Режим торможения

Затормозить развитие сетей пятого поколения может отсутствие коммерческого оборудования, а также необходимость значительных вложений для создания инфраструктуры

«Сейчас главный минус связи пятого поколения — в отсутствии единого понимания стандартов, из-за чего комплексное развитие IOT-рынка заторможено. Сегодня сети 5G — предмет манипуляций и больших ожиданий. Некоторые компании уже предлагают мобильные телефоны, работающие на стандартах 5G, но самого стандарта развертывания как такового в России еще нет. В то же время свои собственные попытки предложить коммерческому заказчику оборудование, поддерживающее 5G, регулярно предлагают, например, мобильные операторы. Здесь ведь как в любой инновации: чем раньше запустишь продукт, тем больший сегмент рынка захватишь», — объясняет Виталий Тепляшин.

По оценкам PWC, объем необходимых капитальных затрат в 2020–2027 годах на строительство сети радиодоступа и модернизации последних миль транспортной сети для одного оператора в среднем составляет порядка 110 млрд рублей, суммарные затраты отрасли достигнут 400–445 млрд рублей при дополнительном сокращении операционных затрат.

«В первое время как в Башкирии, так и в других регионах будет подниматься вопрос бесшовности покрытия — на старте оно может быть точечным и не покрывать всю территорию городов. Для повсеместного использования сети необходимо освободить спектры частот, занятые сейчас спутниковой связью или гражданскими службами в других целях. Операторам необходимо в оперативном режиме обновить всю сетевую инфраструктуру, установив базовые станции и другое оборудование с поддержкой 5G», — считает руководитель отдела инновационного развития компании-интегратора ИТ-сервисов Orange Business Services Антон Козлов.

В то же время региональные телеком-операторы отмечают, что проблемы для них в обновлении сетей нет. «Сеть модернизируется в регионе достаточно активно. Технологии сейчас настолько совершенны, что обновление сети можно сделать на уровне софта. Мы обновляем софт, закупаем определенные лицензии на это, и все — работает обновленное оборудование, поддерживающее высокие скорости. Мы буквально в этом году уже запустили LTE сети, и показатель скорости — 967 мегабит в секунду. Это говорит о том, что мы идем достаточно системно, обновляем устаревшее оборудование, модернизируем его, добавляем новые базовые станции», — объясняет директор компании МТС в Башкирии Антон Марченко.

Сдерживающим фактором, как отмечают в PWC, может выступить также необходимость обновления устройств пользователей для подключения к данной технологии. Антон Козлов также считает, что главная сложность, с которой столкнутся пользователи — ограниченное число абонентских устройств на старте. «Сейчас 5G поддерживает лишь один смартфон, доступный в широкой продаже — Samsung Galaxy S10. Через несколько месяцев появятся и другие устройства с 5G модулем, включая Samsung Fold и телефон от Huawei (модельный ряд Honor)», — отмечает он.

По данным компаний «Ростелеком» и «МегаФон, запуск сети сотовой связи пятого поколения будет реализован до третьего квартала 2019 года, коммерческий запуск 5G назначен до 2022 года.

Лида Богатырева

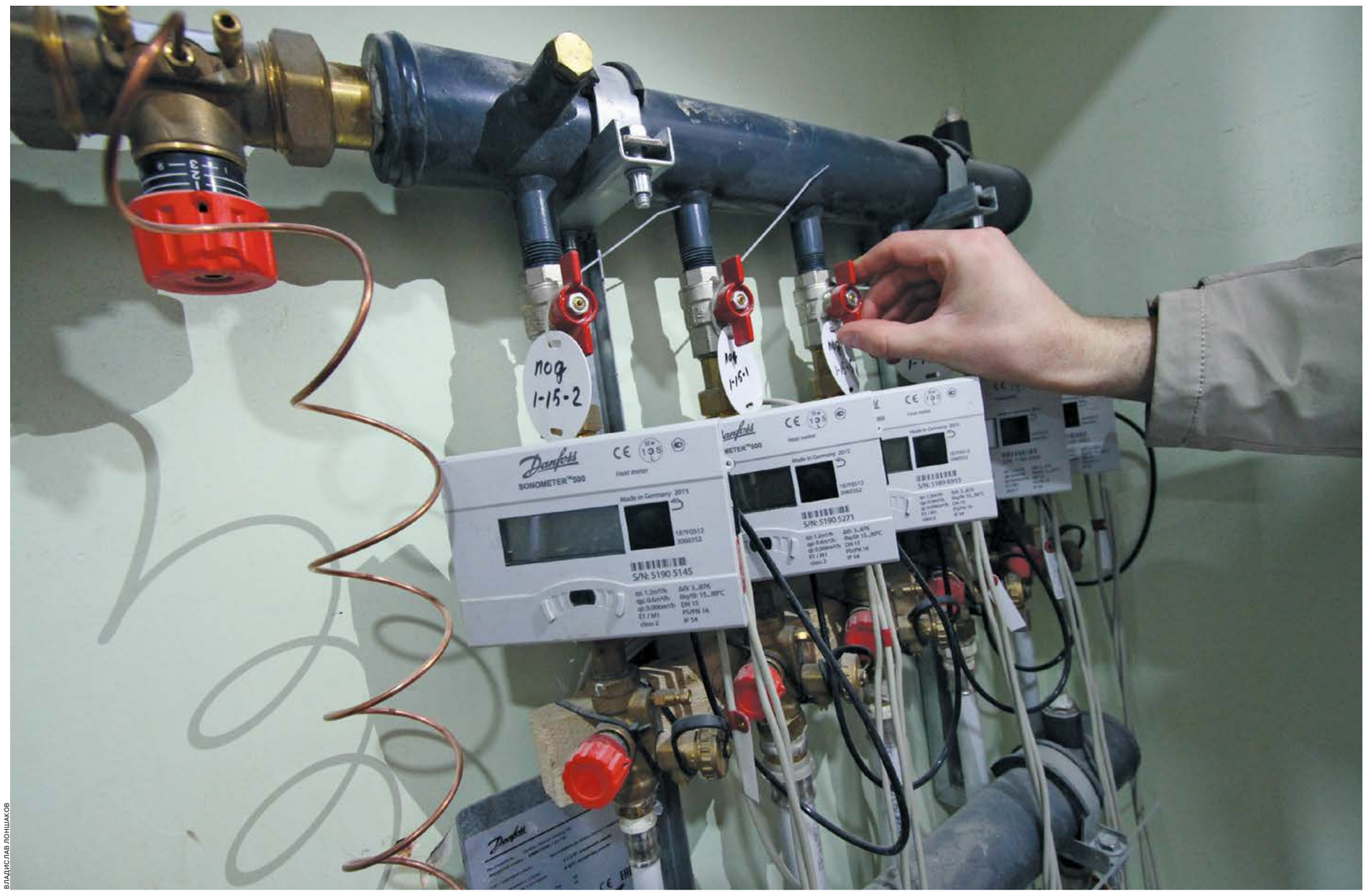
информационные технологии

ЖКХ перейдет на цифру

с13 Требование вступит в силу не ранее 1 июля 2019 года и будет касаться новостроек, а также домов с капремонтом. Условия для внедрения умных счетчиков планируется разработать к концу 2019 года. К концу 2021 года их будут использовать во всех новостройках, а также в половине домов, где приборы учета заменят в ходе капремонта в 2020–2021 годах.

В Башкирии пилотный проект по автоматическому снятию данных с приборов учета в режиме онлайн запущен в марте 2018 года. Счетчики оснащены антивандальным предохранителем, выявляющим все попытки воздействия на устройство. Проект пока что реализован только в нескольких домах в Благовещенске. Установку счетчиков газа, света и воды профинансировали управляющие компании (УК, — прим. «ИТ»), сумма затрат на каждую УК составила 150 тыс. руб.

Заместитель директора по развитию VAS-продуктов (от англ. Value Added Services — услуги, приносящие дополнительный доход, — прим. «ИТ») и сервисов компании «Инфосистемы Джет» Денис Гараев считает, что ситуация с внедрением цифровых систем в ЖКХ в регионе складывается благополучно. По его словам, федеральные и локальные компании внедряют цифровые решения по учету ресурсов, а это значит, что в скором времени сфера жилищно-коммунального хозяйства перейдет на «цифру».



ВЛАДИСЛАВ ЛОНЩАКОВ

Примеры умных систем ЖКХ в Башкирии есть, но эксперты называют их ненадежными

Телеком готов

В процессах цифровизации сферы ЖКХ наиболее активно участвуют телекоммуникационные компании, у которых есть ресурсы для сбора, хранения, обработки и передачи данных. В Башкирии телекомоператоры имеют готовые решения для «умного» ЖКХ, в частности, беспроводные сети передачи данных со счетчиков на дальние расстояния.

По словам директора филиала АО «ЭР-Телеком Холдинг» (ТМ «Дом.ru Бизнес», «Дом.ru») Ольги Карелиной, в республике компания построила часть IoT-сети, которая базируется на технологии LoRaWAN. «Преимущество IoT-сети — возможность быстрого масштабирования, доступная цена цифровых решений для массового применения и возможность автономной работы IoT-датчиков до 10 лет. Это позволяет оцифровывать городскую среду и внедрять цифровые решения, в том числе в отрасли ЖКХ. В 2019 году запущен совместный проект с администрацией Уфы. В административных зданиях установлены «умные» счетчики электроэнергии и воды, датчики температуры, влажности, протечки, а также датчики дыма. Данные передаются беспроводным способом по сети LoRaWAN и выводятся на единую приборную панель, что позволяет автоматизировать процесс сбора достоверных показаний, осуществлять онлайн-мониторинг микроклимата рабочих помещений и контроль возникновения чрезвычайных ситуаций. Также «ЭР-Телеком Холдинг» начал внедрять «Умные домофоны». Устройства снабжены камерой видеонаблюдения и обеспечивают ряд дополнительных возможностей. Так, подключив мобильное приложение «Умный Дом.ru», жители имеют возможность принимать звонки с домофона на смартфон, удаленно открывать дверь в свой подъезд или двор, видеть изображение с камеры домофона в режиме реального времени. Проект уже запущен в 25 городах, в том числе в Уфе», — рассказала она.

В поволжском филиале ПАО «МегаФон» отметили, что у компании есть работающая система для ЖКХ в домах Иннополиса в Татарстане, где показания учета собирают «умные» счетчики на основе стандарта NB-IoT (Narrow Band Internet of Things — узкополосный интернет вещей, когда данные с датчиков отправляются непосредственно на главный сервер, — прим. «ИТ»). Это автоматизированная система сбора и передачи показаний приборов учета — веб-интерфейс, который дает возможность отслеживать потребление ресурсов, автоматически собирать и передавать данные в службы ЖКХ, просматривать их в защищенном облачном интерфейсе. Система позволяет предприятиям ЖКХ и управляющим компаниям получать информацию о потреблении ресурсов, а жителям не нужно снимать показания вручную. К преимуществам можно также отнести возможность отслеживать состояние оборудования и вести учет расходов. Представители телеком-оператора добавили, что в этом году развернули такую же сеть и в Башкирии.

Компания МТС также запустила сеть для интернета вещей NB-IoT. Решения IoT МТС выступают как основа эффективного управления городом и оптимизации расхода ресурсов ЖКХ. МТС выступает поставщиком вертикальных IoT-решений, инфраструктуры радиодоступа и M2M-коммуникаций. Примеры использования в области умного города и ЖКХ — региональные электросетевые и водоснабжающие компании, УК, общедомовой учет, котельные, лифты, пассажироперевозки. Подробности запуска сети NB-IOT — во вложении. В настоящее время сеть интернета вещей доступна во всех городах Башкирии (до 50 тыс.).

Регион с запросом

Башкирия готова к изменениям в сфере ЖКХ и видит в применении «умных» технологий выгоду. Для сетей NB-IoT и LoRaWAN характерна установка устройств приема и передачи данных в труднодоступных местах, низкая стоимость и энергопотребление. По задумке применение «умных» систем в ЖКХ исключает незаконные подключения к коммуникациям, ошибки при снятии показаний, неисправные или устаревшие приборы учета — все это в конечном итоге может привести к удешевлению коммунальных услуг.

Однако, чем быстрее идут процессы цифровизации в сфере ЖКХ, тем актуальнее становятся угрозы безопасности.

«Первая проблема безопасности ЖКХ в регионе состоит в том, что в большинстве своем решения имеют сырую архитектуру и при их создании разработчики не обращают внимания на соблюдение стандартов по информационной безопасности. Более того, большинство оставляет для себя возможность удаленного подключения для управления устройствами, обновления версий установленного программного обеспечения. Отсутствие соблюдения стандартов безопасности порождает наличие большого количества уязвимостей и возможностей для взлома», — считает Александр Оводов.

Вторая проблема, по словам господина Оводова, кроется на этапе проектирования вновь создаваемых и модернизируемых систем в рамках перехода на цифру. «Как правило, при проектировании таких систем не закладываются решения, позволяющие снизить или полностью исключить возможность эксплуатации имеющихся в цифровых устройствах и системах уязвимостей, — отмечает эксперт. Злоумышленники это прекрасно знают и этим пользуются. На каждом уровне цифрового ЖКХ могут быть свои последствия от действий злоумышленников. Если это умные счетчики, то злоумышленники (даже школьники) могут «скручивать» или «накручивать» их показания. Умные лампочки могут выдать миганием на нечувствительной для глаз человека частоте злоумышленникам логины и пароли от Wi-Fi. Цифровые замки дают возможность открыть дверь, розетки — оставить вас без электричества; умное отопление и кондиционер — отпустить или поднять температуру до критических отметок. На уровне управления и мониторинга систем тепло-, водо-, электроснабжения могут быть и более серьезные последствия — от прекращения снабжения до техногенных аварий с серьезными финансовыми потерями и даже человеческими жертвами».

По мнению экспертов консалтинговой компании PWC, для программы безопасности в киберпространстве IoT нужна оптовая закупка новых технологий и решений. Огромное количество идентификационных записей в экосистеме IoT потребует наличия единообразного подхода к авторизации и лишения доступа к данным, важна также надежная аутентификация пользователей, чтобы защитить подключенные устройства, на которых хранятся или передаются конфиденциальные данные. Александр Оводов считает, что для защиты ресурсоснабжающим организациям и владельцам котельных необходимо строить систему защиты совей информационной инфраструктуры согласно требований 187-ФЗ «О безопасности критической информационной инфраструктуры». Для управляющих компаний эксперт порекомендовал при построении системы защиты умных зданий ориентироваться на CIS Critical Security Controls от SANS Instituite и регулярно проводить внешние аудиты информационной безопасности. При выборе производителей решений по автоматизации запрашивать наличие документов, подтверждающих независимую проверку исходного кода на наличие уязвимостей. «Для граждан, которые хотят превратить свой дом в умный, лучше обращаться к специалистам по информационной безопасности, не доверяя тому, что говорят продавцы», — отметил он.

Лида Богатырева

БУДУЩЕЕ ТЕХНОЛОГИЧНО

Факультет информатики и робототехники (ФИРТ) в Уфимском государственном авиационном техническом университете (УГАТУ) объявляет набор абитуриентов, 450 из которых могут поступить на бюджет.

ПРАКТИЧНОЕ ОБУЧЕНИЕ

«Выпускники ФИРТ сейчас становятся все более востребованными на рынке труда. Профессорско-преподавательский состав готовит студентов не только к профессиональной карьере в области IT-технологий, но и помогает поднять уровень своих знаний и навыков, достичь руководящей высокооплачиваемой должности в сфере информационных технологий. Наши выпускники успешно устраиваются на работу в ведущие производственные предприятия и фирмы», — отметили представители университета.

К примеру, кафедра геоинформационных систем (ГИС) работает над коммерциализацией научно-исследовательских работ, внедряет геоинформационные технологии на предприятиях реального сектора экономики. К таким можно отнести ОАО «Газпром Газораспределение Уфа», ПАО АНК «Башнефть», ОА «Транснефть-Урал».

В качестве еще одного примера взаимодействия с предприятиями сектора экономики, банками и силовыми структурами можно привести работу кафедры финансов, денежного обращения и экономической безопасности (ФДОиЭБ). Ее преподаватели — руководители подразделений крупных банков, государственных органов, финансовых и аудиторских компаний.

Перспективы для студентов ФДОиЭБ также открываются после участия в студенческих олимпиадах по экономической безопасности, рынку ценных бумаг в Москве, Санкт-Петербурге. В 2018 году команда студентов ФДОиЭБ заняла первое место на студенческом конкурсе «Лучший инвестор на финансовом рынке», проводимом при поддержке ОА ИФК «Солид». Помимо этого, есть возможность стать частью проектов «Школы экономической дипломатии в развитии евразийской интеграции».

Студенты кафедры вычислительной техники и защиты информации ВТиЗИ могут принять участие в различных мероприятиях, посвященных информационной безопасности. В 2018 году кафедра была награждена дипломом лауреата в номинации «Образовательный центр года», а студент-выпускник специальности «Безопасность информационных технологий в правоохранительной деятельности» удостоен золотой медали конкурса на лучшую научную работу студентов в области информационной безопасности.

Тесно сотрудничает с предприятиями и кафедра технической кибернетики (ТК), осуществляющая подготовку по направлениям «Системный анализ и управление», «Управление в технических системах» и «Управление качеством». В частности, 28 марта 2019 года студенты кафедры ТК заняли призовые места в международной олимпиаде по основам автоматизации управления в технических системах. Студенты кафедры ТК ежегодно принимают участие в Всероссийской олимпиаде «Я — профессионал» и становятся призерами олимпиады по направлениям «Робототехника» и «Программная инженерия».

ВЫБОР БУДУЩЕГО

На факультете есть несколько направлений бакалавриата (срок обучения четыре года), три специальности (срок обучения пять лет) и десять направлений магистратуры.

Направление бакалаврской подготовки «Математическое обеспечение и администрирование информационных систем» дает выпускникам возможность разрабатывать математические модели, алгоритмическое и программное обеспечение, работать с различными техническими системами.

Бакалавры, окончившие специальность «Программная инженерия», смогут работать на индустриальном производстве программного обеспечения для разных информационно-вычислительных систем.

Выпускники направления «Бизнес-информатика» — это будущие IT-менеджеры, которые понимают информационную инфраструктуру компании и разбираются в бизнесе на уровне высшего руководства.

Студенты «Информационных систем и технологий» смогут проектировать, разрабатывать и эксплуатировать информационные системы, алгоритмы обработки.

Бакалавры «Прикладной информатики» могут получить работу в сфере информационных технологий промышленных, государственных, коммерческих и финансовых организаций и банков.

Специальность «Применение и эксплуатация автоматизированных систем специального назначения» предназначена для подготовки специалистов по созданию и эксплуатации автоматизированных систем реального времени.

Направление «Информационная безопасность» готовит бакалавров для работы с нормативными правовыми актами в области защиты информации, выявления угроз безопасности информационным системам, программно-аппаратной защиты информации, а также методами тестирования на проникновение в современные компьютерные системы.

Студенты, закончившие специальность «Безопасность информационных технологий в правоохранительной деятельности», одинаково хорошо разбираются в информационной безопасности, в психологических методах воздействия и нормативно-правовой базе РФ, а также в специфичных науках, например, в криминалистике.

Профессиональная деятельность выпускников направления «Информатика и вычислительная техника» связана с проектированием, разработкой, обеспечением и развитием сложных программных систем, разработкой широкого спектра вычислительных устройств — от небольших контроллеров до суперЭВМ, локальных и глобальных вычислительных систем, а на «Экономической безопасности» готовят специалистов в области права, финансов, психологии, информационных технологий.

Студенты «Специальных организационно-технических систем» смогут решить сложные задачи управления бизнес-процессами в проектировании, планировании, прогнозировании, оперативном и стратегическом управлении, реинжиниринге организационных и технических систем на основе современных компьютерных технологий и компьютерного моделирования.

«В 2018 году все направления подготовки бакалавров и магистров, а также специальности Факультета информатики и робототехники прошли аккредитацию. Наши студенты побеждают и занимают призовые места в престижных всероссийских конкурсах и олимпиадах. Они награждаются стипендиями Президента РФ и Правительства РФ, именными стипендиями», — подчеркнули в университете.

Уфа, К. Маркса, д. 12, к. 6, каб. 418
+7 (347) 273-77-17
dekanat.firt@gmail.com

РЕКЛАМА