Развитие фиксированного беспроводного доступа (FWA) в сельской местности

Дочерняя компания ТОО «Ауыл Телеком» реализует пилотные проекты по развитию фиксированного беспроводного доступа (FWA) в сельской местности, обеспечивая высокоскоростной интернет там, где строительство ВОЛС или GPON экономически нецелесообразно. Это позволяет снизить цифровое неравенство и предоставить современную связь жителям отдаленных регионов.

В рамках пилотных проектов уже протестированы решения на базе Open RAN и FWA 5G. В селе Сарыбай средняя скорость соединения выросла в 85 раз — с 5 Мбит/с до 427 Мбит/с, что позволило значительно улучшить качество онлайн-образования, телемедицины и удаленной работы. Таким образом, FWA не только обеспечивает модернизацию устаревших технологий (WiFi, ADSL, CDMA EVDO), но и становится ключевым инструментом для устранения цифрового разрыва между городом и сельской местностью.

Компания «Ауыл Телеком» продолжает активно расширять сеть FWA, причем 5G является стратегическим направлением для компании. Однако параллельно строится и сеть 4G. Примером успешной реализации является село Каратала Актюбинской области, где подключено 79 домохозяйств из 120. Средняя скорость соединения составляет 46 Мбит/с, а среднее потребление интернет-трафика на одно домохозяйство за 3 недели достигло 191 ГБ. У 10 абонентов объем потребления превысил 450 ГБ за тот же период.

Тестирование различных сетевых функций и технических решений

- Протестирована техническая возможность и готовность программно-аппаратного комплекса на базе Open RAN 5G Fronthaul для предоставления доступа в Интернет по фиксированному беспроводному доступу. Работоспособность ПАК Open RAN 5G Fronthaul подтверждена с некоторыми ограничениями.
- Протестирован программный комплекс invGUARD AS-SW для определения его возможностей по мониторингу и анализу статистики сетевого трафика на сети АО «Казахтелеком» в облачной среде TelcoCloud.
- Протестирована технология VOLTHA GPON в облачной среде TelcoCloud в г. Конаев. Основная идея данного решения — дезагрегация и уход от вендорной зависимости. В классическом GPON оборудование OLT (стационарное), ПО, лицензии и ONT (клиентское) поставляются одним вендором и «залочены», что не позволяет подключать ONT других производителей к OLT другого вендора или использовать ПО других вендоров. Решение VOLTHA позволяет обойти эти ограничения: идея заключается в возможности выбирать оборудование (white-box оборудование OLT) у одного производителя, ПО и лицензии — у другого, а внедрение стандарта openOMCI позволяет подключать ONT различных вендоров.
- Продукт еще не полностью готов, но сама идея и активность уже приносят результаты. Пилотный проект ШПД на базе VOLTHA в г. Конаев в стадии реализации.
- Протестирована услуга предоставления доступа к кэш серверам для операторов связи РК и Центральной Азии.
- Запущено тестирование indoor-решения по обеспечению мобильного доступа в интернет посредством PicoCell в местах с плохим качеством мобильной связи/ШПД (магазины, кафе в подвальных помещениях).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ

Компания осознает важность обеспечения информационной безопасности и защиты данных своих клиентов. В АО «Казахтелеком» продолжается развитие надежной системы управления информационной безопасностью и защитой данных.

ПОДХОД К УПРАВЛЕНИЮ

GRI 3-3, 418-1

Служба информационной безопасности — в непосредственном подчинении у Управляющего директора по информационной безопасности, которая контролирует вопросы информационной безопасности в Компании на верхнем уровне.

Основными внутренними документами, регулирующими вопросы в области информационной безопасности, являются:

- Политика информационной безопасности.
- Политика по защите персональных данных в АО «Казахтелеком».
- Концепция по информационной безопасности.

С документами Компании, регулирующими вопросы в области информационной безопасности, можно ознакомиться на сайте компании в разделе «Устойчивое развитие», подраздел «Информационная безопасность и защита данных».

Основные принципы обеспечения информационной безопасности:

- исполнение законодательных норм;
- вовлеченность высшего руководства Компании в процесс обеспечения ИБ;
- ориентированность на бизнес;
- процессный подход;
- комплексное использование способов, методов и средств защиты информации;
- следование лучшим практикам;
- разумная достаточность;
- информированность и персональная ответственность.

Для обеспечения информационной безопасности АО «Казахтелеком» применяет системный подход. Одним из важных аспектов является круглосуточный контроль данных на всех этапах их жизненного цикла, начиная с момента их поступления в инфраструктуру Компании и заканчивая их архивацией или безвозвратным уничтожением.

На данный момент в Компании используются лучшие мировые практики методов обеспечения информационной безопасности. Наши внутренние системы защищены с помощью таких решений, как безопасный удаленный доступ к информационным ресурсам, безопасное использование интернета, контроль привилегированных пользователей (PAM), сканеры уязвимостей и другие. Компания стремится противостоять внешним угрозам и внедряет новые решения и методы работы с ресурсами, включая создание необходимой инфраструктуры в Компании, обучение квалифицированных специалистов, формирование оперативного центра информационной безопасности и внедрение концепции ZeroTrust.

Также в Компании используются такие важные элементы безопасности, как встраивание в государственную систему кибербезопасности ЕШДИ, безопасность Интернета вещей, использование ловушек Honeypot, Machine Learning и другое. Кроме того, на постоянной основе проводится обучение и повышение ИБ-осведомленности сотрудников Компании.

Защита персональных данных

GRI 418-1

В Компании разработана и внедрена «Политика защиты персональных данных», в которой определены основные принципы обработки персональных данных клиентов, поставщиков, деловых партнеров, работников и других лиц, а также определены основные действия по сбору, хранению и обработке персональных данных, а также меры по их защите.

Политика является основополагающим документом в области защиты персональных данных, устанавливает цели, задачи и принципы в области защиты ПД, которыми руководствуется Компания в своей деятельности. Служит руководством при разработке соответствующих документов защиты персональных данных.

Основные принципы обеспечения защиты персональных данных:

- соблюдение конституционных прав и свобод человека и гражданина;
- законность обеспечения защиты персональных данных;
- конфиденциальности персональных данных ограниченного доступа;
- вовлеченность руководства Компании в процесс обеспечения защиты персональных данных;
- ориентированность на бизнес;
- процессный подход;
- комплексное использование способов, методов и средств защиты;
- следование лучшим практикам;
- разумная достаточность;
- информированность и персональная ответственность.

Основные результаты за отчетный период

В области информационной безопасности в 2024 году в Компании проведен комплекс мероприятий для обеспечения защиты корпоративных информационных систем, персональных данных, служебной информации и сетей передачи данных.

В рамках поддержания в актуальном состоянии системы управления информационной безопасности в Компании утверждены 16 нормативно-регламентирующих документов.

В рамках повышения уровня осведомленности работников АО «Казахтелеком» в области обеспечения информационной безопасности произведено 7 рассылок информационных материалов, запущено 2 цифровых марафона на базе обучающего портала Корпоративного университета о правилах и требованиях информационной безопасности, а также проведено 4 киберучения в виде рассылки фишинговых писем, для оценки осведомленности работников в области кибергигиены, а также отработки действий пользователей при получении подозрительных писем.

Произведена комплексная проверка объектов/серверных помещения с оборудованием Компании, отнесенным к КВОИКИ, а также структурные подразделения, сопровождающие/администрирующие данное оборудование. По выявленным несоответствиям руководителям структурных подразделений филиалов выданы рекомендации.

В части оперативной работы по информационной безопасности в 2024 году Дивизион ИТ реорганизовал работу подразделений, для запуска корпоративного Оперативного центра информационной безопасности (ОЦИБ) и перевода в режим работы 24/7. В основные обязанности входит:

- Защита корпоративного периметра Компании;
- Мониторинг событий информационной безопасности (ИБ);
- Реагирование на инциденты ИБ;
- Расследование инцидентов ИБ;
- Поиск уязвимостей в информационных системах Компании;
- Выдача рекомендаций по устранению инцидентов информационной безопасности;
- Контроль средств защиты информации (СЗИ).

В 2024 году реализован второй этап перехода Компании к модели ZeroTrust, произведено внедрение ряда программно-аппаратных средств защиты информации (СЗИ), что позволило усилить имеющуюся защиту корпоративной инфраструктуры Компании. Результаты работы корпоративного ОЦИБ:

- отражено порядка 3 300 DDOS атак на ресурсы клиентов (пиковая величина более 74 Гбит/сек), общим трафиком свыше 1 100 Тбит;
- заблокировано более 710 млн пакетов вредоносного трафика;
- Сканерами уязвимостей программного обеспечения (ПО) выявлено порядка 118 тысяч уязвимостей эксплуатируемого в Компании ПО, и устранено ответственными администраторами свыше 64 %;
- Посредством СЗИ отражено более 40 тысяч сетевых атак, обнаружено 45 тысяч вирусов, заблокировано свыше 20 тысяч попыток подбора пароля;
- Контролируется при помощи PAM (Privileged Access Management – система контроля привилегированных пользователей) более 270 привилегированных пользователей (администраторов информационных систем, внешних пользователей и подрядчиков) на свыше 120 ip-адресов терминальных серверов Корпоративных информационных систем;
- Обнаружено при помощи DLP (Data Leak Prevention – предотвращение утечек данных) более 800 файлов с конфиденциальной информации, хранящиеся с нарушением требований ИБ;
- Развернуто порядка 60 ловушек (Honeypot – полностью имитирующих информационные системы/ресурсы Компании), которые позволили выявить более 2 000 зловредных запросов внутри корпоративной сети Компании.

В отчетном периоде было зафиксировано одно обращение по горячей линии касательно возможного нарушения обработки персональных данных клиента. Факт утечки данных клиента не подтвержден.
В отчетном периоде в Компании не было выявлено фактов утечки данных клиентов.

Информирование и обучение сотрудников по вопросам информационной безопасности

GRI 418-1

В Компании на постоянной основе проводятся обучающие мероприятия серди сотрудников для обеспечения основных принципов информационной безопасности – конфиденциальности, целостности и доступности данных.

Информационная безопасность обеспечивается как на административном уровне – каждый сотрудник обязан ознакомиться и исполнять требования регламентов, правил, политик Компании в области информационной безопасности, так и на техническом и физическом уровне – в компании используются различные аппаратно-программные комплексы, средства криптографической защиты информации и прочее.

Кроме того, специалисты Дивизиона ИБ регулярно проходят различные курсы повышения квалификации по информационной безопасности, кибербезопасности, рискам и угрозам ИБ.
Для сотрудников подразделений по работе с клиентами и по работе с персоналом, где риск неправомерного использования данных достаточно высокий, проводится общее обучение/тестирование по цифровой гигиене.