UZTELECOM

Обеспечение безопасности личных данных и информации является нашим главным приоритетом.

Политика информационной безопасности, реализуемая Компанией, основана на международных стандартах и лучших практиках отрасли. Мы внедряем в наши сети современные технологии безопасности и регулярно совершенствуем их. Обеспечение безопасности, конфиденциальности и целостности данных наших абонентов и партнеров является одной из наших основных задач.

Для обеспечения безопасности данных абонентов в компании разработана Политика информационной безопасности, в которой изложены принципы, подходы и меры, позволяющие надежно защитить данные и соблюдать стандарты, установленные в области безопасности.

Политика информационной безопасности АК “Узбектелеком”

Акционерная компания “Узбектелеком” (далее - Компания) является крупнейшим оператором телекоммуникаций, сеть которого охватывает все регионы Республики Узбекистан. Используя телекоммуникационную сеть, построенную на основе современных технологий, Компания предоставляет все виды телекоммуникационных услуг.

Компания эффективно внедряет и использует в своей деятельности высокотехнологичную информацию и коммуникации. В таких условиях обеспечение информационной и кибер-безопасности является необходимой задачей.

Учитывая важность информационной безопасности, данное направление выделено в качестве одной из основных функций заместителя председателя правления АК “Узбектелеком” по информационной безопасности и режиму. Информационная безопасность достигается путем внедрения и реализации ряда мер, таких как установка соответствующего оборудования и программного обеспечения, проведение тестов для выявления уязвимостей в сетях, организация обучения сотрудников, регулярный мониторинг систем. Комплексные меры по обеспечению информационной безопасности позволяют обеспечить бесперебойную работу сетей Компании, минимизировать ущерб от угроз, обеспечить конфиденциальность и защиту персональных данных абонентов, защитить информационно-коммуникационную инфраструктуру от различных угроз, прогнозировать и предотвращать воздействие угроз, поддерживать деловую репутацию и соответствовать требованиям, установленным законодательными документами.

Политика информационной безопасности компании разработана на основе следующих документов:

Закон Республики Узбекистан от 2 июля 2019 года № 547 “О персональных данных”;

Закон Республики Узбекистан от 15 апреля 2022 года № 764 “О кибербезопасности”;

Постановление Президента Республики Узбекистан от 5 октября 2020 года № ПФ-6079 “Об утверждении стратегии “Цифровой Узбекистан – 2030” и мерах по ее эффективной реализации”;

Постановление Президента Республики Узбекистан от 31 мая 2023 года № PQ-167 “О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан”;

Постановление Кабинета Министров Республики Узбекистан от 5 октября 2022 года № 570 “Об утверждении некоторых нормативных правовых актов в области обработки персональных данных”;

Uz DSt ISO/IEC 27000:2022 “Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Комментарии и глоссарий”;

Uz DSt ISO/IEC 27001:2020 “Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования”;

Uz DSt ISO/IEC 27002:2016 “Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью”;

Внутренние нормативные документы, разработанные компанией, соответствующие планы действий.

Цели и задачи

Основными целями Политики информационной безопасности Компании защита субъектов информационных отношений от материального, физического, морального и иного вреда, случайного или умышленного несанкционированного вмешательства в деятельность объектов информатизации или несанкционированного доступа и неправомерного использования содержащейся в них информации, устранение и минимизация возможных последствий инцидентов информационной безопасности, прогнозирование и предотвращение угроз, выявление и устранение уязвимостей в информационных системах, обеспечение выполнения требований, установленных законодательными документами, инструкциями и нормативными документами в области информационной безопасности, обеспечение резервирования и восстановления информационных ресурсов Компании.

Важнейшей задачей является предотвращение и обнаружение несанкционированного доступа к информационным объектам Компании, выявление и устранение уязвимостей в информационных ресурсах Компании и системах управления информационной безопасностью, обеспечение внимательного отношения всех сотрудников компании к информационной безопасности, предоставление информации о любых потенциальных угрозах, сохранение в тайне конфиденциальной информации и коммерческой тайны, а также персональных данных клиентов.

Сегодня компания работает не только в области информационной безопасности и кибербезопасности, но и обеспечивает безопасность вас и ваших близких. Примером тому служат услуги Компании “Безопасность ребенка”, “Dr.Web - антивирусное решение”.

Меры информационной безопасности

Внутренние нормативные документы Компании в области информационной безопасности разрабатываются и поддерживаются Департаментом безопасности Компании. Внутренние нормативные документы по информационной безопасности и требования, изложенные в них, доводятся Департаментом безопасности до всех сотрудников Компании, и сотрудники работают в строгом соответствии с установленными требованиями.

В Компании регулярно проводится соответствующая работа по защите и неразглашению конфиденциальной информации, созданию и развитию систем и средств защиты информации, повышению квалификации и осведомленности сотрудников в области информационной безопасности.

Отдел безопасности Компании следит за выполнением задач, возложенных на администраторов корпоративных сетей, систем и информационной безопасности.

Служба безопасности Компании ежеквартально организует работы по инвентаризации средств защиты информации в локальных сетях и на компьютерах на рабочих местах сотрудников, которые проводятся в рамках внутренних аудитов. Если по результатам инвентаризации необходимо принять соответствующие меры, проводятся необходимые работы.

Регулярно проводится мониторинг данных корпоративной электронной почты, данных официального сайта, настроек и данных файлового сервера, контроллера домена главного сервера, настроек и баз данных средств информационной безопасности в информационных системах и ресурсах Компании.

Для обеспечения надежности (безопасности) данных информационной системы используются RAID-системы хранения данных основного и резервного центров обработки данных.

Для обеспечения физической защиты данных серверы баз данных и системы хранения данных расположены в защищенном серверном помещении в Центре обработки данных компании (DataCentre).

Соглашения о неразглашении подписываются с сотрудниками, с которыми заключены трудовые договоры, а также с партнерами, с которыми заключены договоры на оказание услуг и соответствующие закупки.

Сотрудники, ответственные за обеспечение информационной безопасности в Компании, регулярно участвуют в различных семинарах и конференциях для повышения своей квалификации в этой области, а также проводится обучение всех сотрудников компании по соблюдению требований Политики информационной безопасности.

Реагирование на инциденты информационной безопасности

Ключевые задачи процесса управления инцидентами информационной безопасности:

Минимизация потерь, включая быстрое обнаружение инцидентов и снижение риска их повторного возникновения;

Оперативное выявление, анализ и регистрация инцидентов информационной безопасности, уведомление уполномоченных органов об инцидентах информационной безопасности, выявление источников и причин инцидентов, рассмотрение их последствий;

Минимизация ущерба информационным ресурсам компании, предотвращение разглашения абонентских данных, восстановление информационных ресурсов, корпоративной сети и информационных ресурсов в случае их выхода из строя в результате инцидента информационной безопасности в короткие сроки, а также анализ результатов устранения последствий инцидента информационной безопасности и принятие соответствующих мер;

Компания должна принимать соответствующие меры по предотвращению повторения инцидентов, связанных с информационной безопасностью информационных ресурсов, и проводить необходимые работы совместно с ГП “Центр кибербезопасности” по инцидентам информационной безопасности.

АК “Узбектелеком” постоянно проводит и совершенствует масштабные работы по обеспечению информационной безопасности.

UZTELECOM -

Ваши данные находятся под надежной защитой.