КИБЕРБЕЗОПАСНОСТЬ В ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЯХ РЕСПУБЛИКИ КАЗАХСТАН

Жандос Кулкенов,
главный инспектор
по информационной безопасности
аппарата акима Карагандинской
области

Как известно, сегодня информационно-телекоммуникационная инфраструктура становится важнейшим элементом экономического развития. Без современной доступной телекоммуникационной инфраструктуры невозможно закрепление Казахстана в мировом экономическом и информационном пространстве. Доступность информационно-коммуникационной инфраструктуры является фундаментом для построения цифровой экономики. (постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 «Об утверждении Государственной программы «Цифровой Казахстан»).

Эффективная реализация мероприятий по цифровизации экономики Республики Казахстан будет обеспечена только при обеспечении единства, устойчивости и безопасности информационно-коммуникационных технологий (*далее* – ИКТ), сохранности данных и доверии граждан к процессам, в основе которых лежат решения, основанные на использовании ИКТ.

За последнее десятилетие Казахстан сделал рывок в развитии ИКТ. И в рамках реализации государственных программ по цифровизации учитывалась скорость внедрения данного направления.

Повсеместная автоматизация и внедрение информационных систем требовали соответствующую защиту. Как следует из мирового опыта, автоматизация и цифровая трансформация должны производиться со строгим соблюдением всех стандартов по защите данных и информации.

Анализ реализованных цифровых проектов помог нам обратить пристальное внимание на проблемные вопросы в обеспечении информационной безопасности в нашей стране. Для решения этих задач был создан

отдельный государственный орган, он же «регулятор», – Комитет по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан (сейчас – Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК). Далее была сформирована нормативная правовая база по информационной безопасности, а именно постановление Правительства РК №832 от 20 декабря 2016 года «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (*далее* – ЕТ).

Внесенные изменения в закон об информатизации и утверждение упомянутых единых требований дали возможность привести меры для усиления защиты объектов информатизации в соответствие с законодательством. ЕТ разработаны согласно подпункту 3) статьи 6 Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации» (*далее* – Закон) и определяют требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности. Положения ЕТ, относящиеся к сфере обеспечения информационной безопасности, обязательны для применения государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры.

Согласно пункту 14 главы 2 ЕТ:

Реализацию задач в сфере информатизации в ГО или МИО обеспечивает подразделение информационных технологий, осуществляющее:

1) мониторинг и анализ применения ИКТ;

2) участие в мероприятиях по учету и анализу использования ИКТ-активов;

3) выработку предложений в стратегический план ГО по вопросам информатизации;

4) координацию работ по созданию, сопровождению и развитию объектов информатизации «электронного правительства»;

5) контроль за обеспечением поставщиками предусмотренного договорами уровня качества оказываемых услуг в сфере информатизации;

6) учет и актуализацию сведений об объектах информатизации «электронного правительства» и электронных копий технической документации объектов информатизации «электронного правительства» на архитектурном портале «электронного правительства»;

7) передачу сервисному интегратору «электронного правительства» для учета и хранения разработанного программного обеспечения, исходных программных кодов (при наличии), комплекса настроек лицензионного программного обеспечения объектов информатизации «электронного правительства»;

8) взаимодействие с сервисным интегратором, оператором, ГО, МИО и организациями в части реализации проектов в сфере информатизации при создании архитектуры ГО и реализации сервисной модели информатизации;

9) реализацию требований по ИБ.

Согласно пункту 30 Параграфа 2 ЕТ:

В целях разграничения ответственности и функций в сфере обеспечения ИБ создается подразделение ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определяется **должностное** лицо, ответственное за обеспечение ИБ.

Сотрудники, ответственные за обеспечение ИБ, проходят специализированные курсы в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата.

Немаловажным для развития ИБ в Казахстане было внедрение Концепции кибербезопасности («Киберщит Казахстана») с утверждением плана мероприятий по ее реализации.

Концепции включает в себя два этапа:

первый этап – 2017–2018 годы;

второй этап – 2019–2022 годы.

Целью Концепции «Киберщит Казахстана» является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающих устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

Для достижения целей установленной концепции «Киберщит Казахстана» постановлением Правительства Республики Казахстан от 28 октября 2017 года № 676 был утвержден План мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года. План состоит из 41 пункта, из которых стоит отметить пункты по обновлению образовательных программ как в вузах, так и в общеобразовательных школах, увеличение грантов по специальности «Системы информационной безопасности» на подготовку кадров с высшим и послевузовским образованием, что способствует развитию человеческого капитала и появлению новых специалистов в области информационной безопасности.

Вместе с этим на основании общего регламента будет функционировать организация по защите персональных данных (Data protection agency) в Казахстане. Сейчас «регулятор» по этому вопросу – это тот же самый комитет по информационной безопасности.

Для защиты особо важных объектов было принято постановление Правительства Республики Казахстан от 8 сентября 2016 года № 529 «Правила отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» – КВОИКИ.

Законом об информатизации определен перечень критически важных объектов информационно-коммуникационной инфраструктуры.

В этот перечень вошли объекты инфраструктуры, которые соответствуют не менее чем одному из 4-х критериев. Прекращение их функционирования приводит к чрезвычайной ситуации социального и (или) техногенного характера либо к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории.

Объекты информационно-коммуникационной инфраструктуры относятся к критически важным при соответствии не менее одному из критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-комму-

никационной инфраструктуры (*далее* – критерии) и подлежат внесению в перечень критически важных объектов информационно-коммуникационной инфраструктуры, утверждаемый Правительством Республики Казахстан.

Критерии

• Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную эксплуатацию особо важных государственных объектов, при нарушении функционирования которого будет остановлена деятельность особо важных государственных объектов.

• Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию стратегических объектов, при нарушении функционирования которого будет остановлена деятельность стратегических объектов либо возникает угроза чрезвычайной ситуации техногенного характера.

• Влияние объекта информационно-коммуникационной инфраструктуры на непрерывную и безопасную эксплуатацию объектов отраслей экономики, имеющих стратегическое значение, при нарушении функционирования которого будет остановлена деятельность объектов отраслей экономики, имеющих стратегическое значение, либо возникает угроза чрезвычайной ситуации техногенного характера.

• Влияние объекта информационно-коммуникационной инфраструктуры на обеспечение устойчивого функционирования объекта информатизации «электронного правительства» и иных информационно-коммуникационных услуг, частичное или полное нарушение (прекращение) функционирования которых может привести к чрезвычайной ситуации социального характера.

В своем Послании 2018 года Президент РК Н.А. Назарбаев подчеркивал следующее: «Внедряя новые технологии, государству и компаниям следует обеспечивать надежную защиту своих информационных систем и устройств. Сегодня понятие кибербезопасности включает в себя защиту не просто информации, но и доступа к управлению производственными и инфраструктурными объектами. Эти и иные меры должны найти отражение в Стратегии национальной безопасности Казахстана».

Я как работник данной отрасли вижу перспективы в развитии, которые зависят как от нас, так и от общества в целом. IT-отрасль развивается с огромной скоростью, и Казахстану еще очень многое придется наверстать.

Последний год нам открыл глаза на многое, в том числе и на проблемы и огрехи в области развития IT и информационной безопасности. Конечно, и до этого были крупные инциденты по информационной безопасности, такие как взломы сайтов (дефейс) государственных органов и «случайный» слив документов и справок с портала eGov.kz. Но это был период до пандемии, и вопрос получения государственных услуг в удаленной формате так остро не стоял как сегодня.

Ситуация с пандемией и переходом на удаленный формат работы всех организаций пролила свет на многие проблемы цифровизации, все это заставляет нас быть более собранными и осведомленными в части вопросов кибербезопасности и IT. За последние годы мы все научились пользоваться персональным компьютером, ЭЦП, государственными ресурсами, приложениями на смартфонах и пр., но теперь пора научиться пользоваться этими благами более безопасно.