Лекция 10. Основные правовые принципы информационной безопасности.

Информация является активом, который, подобно другим важным деловым активам, имеет большое значение для бизнеса организации и, следовательно, должен быть адекватно защищен. Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Информационная безопасность достигается посредством реализации соответствующего набора мер контроля, включая политики, процедуры, процессы, организационные структуры и функции программного и аппаратного обеспечения. Политика информационной безопасности (далее — Политика) – комплекс превентивных мер по защите информации, в том числе информации с ограниченным распространением (служебная информация), информационных процессов и включает в себя требования в адрес пользователей информационных систем Министерства энергетики Республики Казахстан, его ведомств и подведомственных организаций в своей деятельности. Политика информационной безопасности Министерства энергетики Республики Казахстан, его ведомств и организации, находящихся в ведении Министерства энергетики Республики Казахстан (далее – Министерство, его ведомства и организации, находящихся в ведении Министерства) разработана на основании Закона Республики Казахстан от 24 ноября 2015 года № 418-V **«Об информатизации»** и постановлений Правительства Республики Казахстан от 14 сентября 2004 года № 965**«О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан».** За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации в центральном аппарате Министерства отвечает департамент информационных технологий и государственных услуг[5].

В ведомствах и подведомственных организациях Министерства должны быть закреплены структурные подразделения и (или) специалист ответственный за обеспечение информационной безопасности. Структурные подразделения и (или) специалист ответственный за обеспечение информационной безопасности проводит необходимые технические и организационные мероприятия, осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Министерстве, его ведомствах и подведомственных организациях. В рамках реализации решения по информационной безопасности создается рабочая группа, задачами которой являются анализ и прогнозирование ситуации в области информационной безопасности, выявление рисков информационной безопасности и прочее. Требования настоящей Политики ***распространяется на все структурные единицы, инфраструктуру Министерства, его ведомства и организации, находящихся в ведении Министерства и обязательны для исполнения всеми сотрудниками и должностными лицами.*** Основные положения Политики распространяются на другие организации, учреждения, осуществляющих взаимодействие с Министерством, его ведомствами и подведомственными организациями в качестве поставщиков и/или

потребителей информации, услуг, и могут применяться для использования во внутренних нормативных, методических документах и договорах [1].

Основными принципами обеспечения информационной безопасности в Министерстве, его ведомствах и подведомственных организациях являются:

– соблюдение требований законодательства Республики Казахстан;

– соответствие международным и национальным стандартам в области информационной безопасности, действующим на территории Республики Казахстан;

– постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей информационных активов;

– выявление причинно-следственных связей возможных проблем и построение на этой основе точного прогноза их развития;

– адекватная оценка степени влияния выявленных проблем на цели Министерства, его ведомств и организаций, находящихся в ведении Министерства;

– эффективная реализация принятых защитных мер;

– наблюдаемость и возможность оценки обеспечения информационной безопасности, результат применения защитных мер должен быть явно наблюдаем (прозрачен) и мог быть оценен специалистом, имеющим соответствующие полномочия;

– классификация обрабатываемой информации, определение уровня ее важности в соответствии с законодательством Республики Казахстан [2].

Основной целью обеспечения информационную безопасность Министерства, его ведомств и подведомственных организаций является:

– предотвращение ущерба её деятельности за счет хищения финансовых и материально-технических средств;

– уничтожения имущества и ценностей;

– разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации;

– нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации, а также предотвращение ущерба сотрудников предприятия.

Целями системы безопасности являются:

– защита прав предприятия, его структурных подразделений и сотрудников;

– сохранение и эффективное использование финансовых, материальных и информационных ресурсов;

– повышение имиджа предприятия за счет обеспечения качества услуг и безопасности пользователей [2].

Политика является основой для:

– выработки и совершенствования комплекса согласованных правовых норм, организационно-административных мероприятий и программно-технических средств защиты информационных ресурсов Предприятия:

– координации деятельности подразделений Предприятия в области обеспечения информационной безопасности;

– ***построения процедур информационного взаимодействия Предприятия с лицами, выступающими в качестве поставщиков информации и услуг.***

Категории информационных ресурсов, подлежащих защите в информационных системах, сопровождение которых осуществляется техническими специалистами всех структурных подразделений Министерства, его ведомств и подведомственных организаций циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, финансовая информация, персональные данные) и открытые сведения.

Защите подлежит информация, содержащая:

- информацию с ограниченным распространением (служебная информация);
- сведения о частной жизни граждан (персональные данные);
- ***общедоступная информация.***

Угрозы информационной безопасности и их источники: Все множество потенциальных угроз по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы — это угрозы, вызванные воздействием на ИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы — это угрозы ИС, вызванные деятельностью человека. Наиболее опасными (значимыми) угрозами информационной безопасности ИС (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих информацию с ограниченным распространением (служебная информация), а также персональных данных;
- нарушение работоспособности (дезорганизация работы) ИС, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов ИС, а также фальсификация (подделка) документов [3].

Основными источниками естественных и искусственных угроз информационной безопасности ИС являются:

- непреднамеренные нарушения (ошибочные, случайные, необдуманные, без злого умысла) установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности и другие действия сотрудников, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих станций, подсистем или систем в целом;
- ***преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.)*** действия сотрудников подразделений, допущенных к работе с ИС, а также сотрудников подразделений, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения информационной безопасности;
- удаленное несанкционированное вмешательство посторонних лиц из телекоммуникационной сети и внешних сетей общего назначения (прежде всего Интернет) через легальные и несанкционированные каналы подключения сети к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам ИС; [4].

Анализ и оценка рисков. Анализ рисков информационной безопасности проводится совместно с работами по инвентаризации и классификации информационных активов Министерства, его ведомств и организациям, находящихся в ведении Министерства. В основе определения и оценки последствий рисков информационной безопасности лежат требования по информационной безопасности к информационным активам и информации, предъявляемые Политикой. Осуществляются следующие действия: идентификация и оценка стоимости технологических и информационных активов; анализ тех угроз, для которых данный актив является целевым объектом; оценка вероятности того, что угроза будет реализована на практике; оценка рисков этих активов. Анализ и оценка рисков должен осуществляться ответственными лицами, назначенными за ведение и обработку

рисков. Ответственные лица определяют риски в отношении своих бизнес процессов, связанные с нарушением конфиденциальности, целостности и доступности информационных активов и информации или иных нарушений. Оценки рисков ***идентифицирует, определяет количество рисков и их приоритеты по отношению к критериям принятия рисков и целям, подходящим Предприятию.*** Риск информационной безопасности определяется как произведение финансовых потерь (ущерба), связанных с инцидентами безопасности, и вероятности того, что они будут реализованы.Оценка рисков информационной безопасности, с точки зрения управления рисками, определяется как анализ систематически подвергающихся угрозам и существующим уязвимостям информационных систем и технологий научными методами и средствами. Оценки рисков должны включать систематический подход определения величины рисков и процесс сравнения оценённых рисков с критериями рисков, с целью их определения значимости (оценка степени рисков). Оценки рисков должны проводиться периодически для реагирования на изменения в требованиях ИБ и в ситуации рисков, например, в активах, угрозах, уязвимостях, воздействиях, оценке степени рисков и при возникновении значительных изменений. В целях получения сравнимых и воспроизводимых результатов эти оценки рисков должны предприниматься методическим образом. Чтобы быть эффективной, оценка рисков ИБ должна иметь чётко определённую область действия и включать взаимосвязь с оценками рисков в других областях, если это целесообразно. Оценка рисков информационной безопасности состоит из трех основных этапов: идентификация угроз, идентификация уязвимостей, идентификация активов.

По результатам оценки определяются приоритеты для управления и внедрения элементов информационной безопасности, действия руководства по обработке соответствующих рисков и решения о расходах на мероприятия, исходящие из возможного ущерба предприятию в результате нарушения информационной безопасности. Оценка рисков должна проводиться систематически для своевременного реагирования на изменения рисков и требований по безопасности. Для оценки рисков и принятия мер, необходимых для управления этими рисками разработана методика по оценке рисков информационной безопасности в ИС Министерства, его ведомствах и организациях, находящихся в ведении Министерства. Область охвата оценки рисков может относиться либо ко всему предприятию, либо к отдельным его частям, конкретным информационным системам, либо к особым компонентам или службам системы, где это практически выполнимо, реально и полезно. Анализ и оценка рисков должны проводиться в соответствии с руководством по реализации стандарта ИСО/МЭК 27001-2008 **«Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования»**. При оценке рисков должно учитываться влияние реализации угроз информационной безопасности на количественные и качественные показатели. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз. Реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе [4].

Информация, предназначенная для публикации в системах общего доступа, должна быть приведена в соответствие требованиям законодательства РК. Для предотвращения несанкционированной модификации, способной привести к значительному ущербу имиджа предприятия, входные данные, предназначенные для публикации, должны быть соответствующим образом проверены и одобрены, а доступ к системе должен быть авторизованным. Информация, введенная в систему

электронной публикации, должна обрабатываться своевременно и точно. Необходимо обеспечить защиту важной информации в процессе ее сбора и хранения. Системы, предоставляющие возможность электронной публикации информации, обратной связи и непосредственного ввода информации, должны находиться под надлежащим контролем [4].

Мониторинг событий информационной безопасности

В целях контроля за реализацией требований настоящей Политики, обнаружения несанкционированных действий по обработке информации и оперативного реагирования ***на выявленные угрозы обеспечивается регулярный мониторинг и регистрация событий информационной безопасности ИС Министерства, его ведомств и подведомственных организаций.*** Мониторинг системы позволяет проводить оценку эффективности применяемых мероприятий по обеспечению информационной безопасности и подтверждать их соответствие требованиям политики доступа. Все соответствующие правовые требования, предъявляемые к мониторингу событий информационной безопасности, должны быть соблюдены в рамках действующего законодательства РК [5]. Должны быть приняты соответствующие меры защиты конфиденциальности. Следует проводить анализ неисправностей для обеспечения уверенности в том, что они были удовлетворительным образом устранены, предпринятые действия надлежащим образом авторизованы, а мероприятия по управлению информационной безопасностью не были скомпрометированы. Мониторинг информационной безопасности должен осуществляться по двум основным направлениям: мониторинг событий нарушения информационной безопасности, поступающих от средств защиты (сетевые атаки, обнаружение вирусов, регистрация попыток несанкционированного доступа и т.д.). Этот вид мониторинга позволяет реагировать и блокировать атаки сразу же по их обнаружению и за счет этого предотвращать или снижать возможный ущерб от их реализации; мониторинг нарушения администраторами и пользователями информационных систем Министерства установленных требований политики информационной безопасности. Этот вид мониторинга позволяет выявлять нарушения до проявления угрозы и принять соответствующие превентивные меры. Основными целями мониторинга информационной безопасности являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных для осуществления:

- контроля за реализацией требований политики информационной безопасности информационных систем Министерства;
- контроля за реализацией положений государственных нормативных актов по обеспечению информационной безопасности в информационных системах Министерства;
- выявления нештатных (или злоумышленных) действий в информационных системах Министерства;
- выявления потенциальных нарушений информационной безопасности;
- ***своевременного выявления и блокирования угроз.***

Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные программные средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п. Дополнительные требования. Обучение и повышение уровня знаний в области информационной безопасности. Необходимо проводить периодическое обучение и повышение квалификации сотрудников Министерства в области информационной безопасности вне зависимости от их территориального местонахождения и без отрыва от рабочего процесса. Обучаемый материал должен быть представлен в простой и понятной форме. Сотрудники должны быть

ознакомлены с мерами ответственности за разглашение информации в соответствии с их функциональными обязанностями, а также с мерами ответственности за возможные нарушения [6, 7].

Список использованной литературы:

1. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешнеполитические перспективы и новые концепты международной стратегии Казахстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан — Лидера Нации. — 2012. — 12 марта. // iwep.kz/index
2. Дмитриенко Т.А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // Информационно-аналитический журнал «ANALYTIC». — 2003. — № — С. 12-14.
3. Стрельцов А.А. Актуальные проблемы обеспечения информационной безопасности // Технологии безопасности. —— № 11. — С.
4. Информация — понятие //wikipedia.org/wiki
5. Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» (утвержден) // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz/
6. Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан. knb.kz/
7. Үмбетәлі Қ.Н. Информационная безопасность республики Казахстан. URL: https://articlekz.com/article/19962