УТВЕРЖДЕНО
Решением Председателя правления
АО «Институт развития
Электроэнергетики и энергосбережения
(Казахэнергоэкспертиза)»
«16» _____ 2024 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ИНСТИТУТ РАЗВИТИЯ ЭЛЕКТРОЭНЕРГЕТИКИ И ЭНЕРГОСБЕРЕЖЕНИЯ (КАЗАХЭНЕРГОЭКСПЕРТИЗА)»

Астана, 2024 г.

Содержание:

Аннотация

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 АО «Институт развития электроэнергетики и энергосбережения» («Казахэнергоэкспертиза») (далее - Общество).

1. Общие положения

Политика определяет основные принципы построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации, информационных ресурсов, объектов информатизации инфраструктуры Общества.

За непосредственную организацию (построение) и обеспечение эффективного функционирования системы зашиты информации в Обществе отвечает специалист по Информационной Безопасности.

Нормативной основой для разработки политики и технической документации по ИБ, является норма пункта 32 «Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

Политика направлена на достижение следующих целей:

- обеспечение непрерывности основных бизнес-процессов Общества;

- минимизация возможных потерь и ущерба от нарушений в области информационной безопасности;

- усовершенствование системы управления информационной безопасности в Обществе.

Политика учитывает современное состояние и ближайшие перспективы развития объектов информатизации, сопровождаемых Обществом.

Соответствие законодательным и договорным требованиям

- С целью определения соответствия состояния ИБ Общества законодательным и договорным требованиями необходимо:

- определить и задокументировать законодательные, нормативные, иные обязательные, договорные требования в отношении ИС:

- разработать и реализовать политику защиты конфиденциальных и персональных данных, соответствующих нормам законодательства;

- проводить анализ состояния информационных активов Общества на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ;

1.1. Нормативные ссылки

В настоящей политике использованы ссылки на следующие нормативные документы:

1. Указ Президента Республики Казахстана от 14 ноября 2011 года «О концепции информационной безопасности Республика Казахстан»;
2. Постановление Правительства Республики Казахстан от 20 декабря 2016 № 832 «Об утверждении Единых требований в области информационно-коммуникационной инфраструктуры обеспечения информационной безопасности»
3. Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 Методы обеспечения защиты свод правил по управлению защиты информаций;
4. Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27001-2008. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
5. Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27002-2009. Методы обеспечения защиты. Свод правил по управлению защитой информации;
6. Государственный стандарт Республики Казахстан СТ РК ГОСТ Р 50739-2006. Средства вычислительной техники. Защита от

несанкционированного доступа к информации. Общие технические требования;

7. Государственный стандарт Республики Казахстан СТ РК ИСО 22301 «Система управления непрерывностью бизнеса».

1.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения информационной безопасности в Обществе являются:

1.соблюдение требований законодательства в области информационной безопасности Республики Казахстан;

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

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

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

5.адекватная оценка степени влияния выявленных проблем на цели Общества, находящихся в ведении Общества;

6.комплексное использование методов и средств защиты компьютерных систем, перекрывающих все существенные каналы реализации угроз и не содержащих слабых мест на стыках отдельных ее компонентов. Защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами. При этом меры, принимаемые для обеспечения информационной безопасности, не должны усложнять достижение уставных целей Общества, находящихся в ведении Общества, а также повышать трудоемкость технологических процессов обработки информации;

7.эффективная реализация принятых защитных мер;

8.гибкость средств защиты для обеспечения варьирования уровнем защищенности в связи с возможными изменениями внешних условий и требований с течением времени;

9.совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем с учетом изменений в методах и средствах перехвата информации и воздействия на их компоненты, нормативных требований по защите, достигнутого этой области опыта других организаций, как отечественных, так и зарубежных;

10. непрерывность принципов безопасного функционирования. Общество, находящихся в ведении Общества должно обеспечивать непрерывность реализации принципов безопасного функционирования.

11. обязательность и своевременность выявления, пресечение попыток нарушения установленных правил обеспечения информационной безопасности. Контроль деятельности пользователей, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей;

12. четкое определение функциональных целей и целей информационной безопасности в документах во избежание неопределенности в организационной структуре, ролей персонала, утвержденных политик и невозможности оценки адекватности принятых защитных мер;

13. определение персональной ответственности за обеспечение безопасности информации и системы ее обработки для каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников должно быть построено таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму;

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

15. классификация обрабатываемой информации, определение уровня ее важности в соответствии с законодательством Республики Казахстан.

1.3. Основные цели обеспечения информационной безопасности

Основной целью обеспечения информационной безопасности Общества является:

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

2. уничтожения имущества и ценностей;

3. разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации;

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

Целями системы безопасности являются:

1. защита прав Общества и сотрудников;

2. сохранение и эффективное использование финансовых, материальных и информационных ресурсов;

3. повышение имиджа Общества за счет обеспечения качества услуг и безопасности пользователей.

Политика является основой для:

1. выработки и совершенствования комплекса согласованных правовых норм, организационно-административных мероприятий и программно-технических средств защиты информационных ресурсов Общества;

2. координации деятельности Департамента Общества в области обеспечения информационной безопасности;

3. построения процедур информационного взаимодействия Общества с лицами, выступающими в качестве поставщиков информации и услуг.

1.4. Кадровая политика по обеспечению информационной безопасности

Функции и обязанности персонала должны быть четко определены в должностных инструкциях и сообщены кандидатам при приеме на работу в Общество.

Сотрудники должны подписать условия трудового договора, в котором установлены их ответственность и ответственность предприятия относительно информационной безопасности.

Сотрудники и представители сторонних организаций, использующие средства обработки информации организации, должны подписать соглашение в соответствии с требованиями информационной безопасности в целях снижения рисков от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации.

Соглашение о соблюдении конфиденциальности и неразглашении подписывается сотрудником или пользователем сторонней организацией до предоставления доступа к средствам обработки информации.

Проверку всех кандидатов на постоянную работу проводит сотрудник кадровой службы в соответствии с действующим трудовым законодательством РК с соблюдением конфиденциальности личных данных. Проверке подлежит следующая предоставляемая кандидатом информация:

1. рекомендации с предыдущих мест работы;
2. резюме претендента;
3. документы об образовании и профессиональных квалификациях;
4. документы, удостоверяющие личность;
5. прочая информация, требующая уточнений.

Информация обо всех сотрудниках, принимаемых в постоянный штат, должна быть собрана и обработана в соответствии с действующим трудовым законодательством РК.

Сотрудники Общества должны быть ознакомлены с требованиями настоящей Политики, правилами и инструкциями по обеспечению информационной безопасности, с обязательным подписанием листа ознакомления, в целях повышения осведомленности, информирования о процедурах реагирования на инциденты и их предотвращения.

Системный администратор выполняет контроль возврата всех активов Общества (средства вычислительной техники, служебные документы, электронные носители и т.д.), находящихся в пользовании сотрудников по окончании действия их трудового договора, а также, в случае использования сотрудником личного оборудования, обеспечить передачу информации руководителю соответствующего подразделения (ответственному специалисту) или удаление информации с оборудования невосстанавливаемыми методами.

Права доступа к информационным системам и ресурсам Общества аннулируются по окончании действия трудового договора (увольнения) сотрудника или подлежат пересмотру при изменении его обязанностей и функций.

Пароли для учетных записей, оставшихся активными, должны быть изменены на момент прекращения трудовой деятельности, вызванной в связи с длительной командировкой, отпуском или окончания действия трудового договора.

1.5. Доступ сторонних организаций к информационным системам

Доступ сторонних организаций к информации и средствам ее обработки должен быть строго регламентирован и контролируемым со стороны руководства и ответственных специалистов Общества.

Там, где есть потребность в доступе третьей стороны к информации и средствам ее обработки (приобретение программных продуктов, сервисное обслуживание и т.д.) следуют провести оценку риска с целью определения возможных последствий и соответствующих мер безопасности, обеспечить их внедрение. Уровень безопасности информации, установленный на предприятии и средств ее обработки при этом не должен снижаться.

Доступ сторонних организаций к информации и средствам ее обработки не должен предоставляться до выполнения соответствующих мер контроля и подписания соглашения об условиях предоставления доступа, требованиях к обеспечению информации, порядке рабочего расположения и ответственности

за его ненадлежащее исполнение согласно законодательным актам о защите данных и прав интеллектуальной собственности.

Специалист по Информационной Безопасности обеспечивает выполнение следующих мероприятий перед предоставлением права доступа сторонним организациям к активам Общества:

1. процедуры по защите активов организации, в том числе информации и программного обеспечения;
2. процедуры для определения компрометации активов;
3. установка ограничений на распространение, дублирование информации;
4. описание предоставляемого продукта или услуги;
5. использование уникальных идентификаторов
6. авторизацию в отношении доступа и привилегий пользователей;
7. меры для отчетности, уведомления о возникновении инцидентов нарушения информационной безопасности;
8. мониторинг и право на аннулирование любых действий, связанные с активами организации.

1.6. Уязвимости основных компонентов информационных систем

Уязвимость – параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними средствами или факторами. Т.е. это некий недостаток в системе, используя который внешний или внутренний злоумышленник, может намеренно нарушить её целостность и вызвать неправильную работу.

Попытки несанкционированного доступа к информации в сети и попытки совершения несанкционированных действий (непреднамеренных и умышленных) могут быть предприняты с рабочих станций сотрудников предприятия.

Оценка уязвимостей – это проверка слабостей, которые могут быть использованы существующими угрозами. Эта оценка должна учитывать окружающую среду и существующие защитные меры. Мерой уязвимости конкретной системы или актива по отношению к угрозе является степень того, с какой легкостью системе или активу может быть нанесен ущерб.

1.7. Пересмотр Политики информационной безопасности

Положения политики информационной безопасности Общества требуют регулярного пересмотра и корректировки не реже одного раза в год согласно плану.

Внеплановый пересмотр Политики безопасности проводится в случае:

1. внесения существенных изменений в ИС Общества, находящихся в ведении Общества;
2. изменениями в законодательстве, организационной структуре Общества, находящихся в ведении Общества;
3. возникновения инцидентов информационной безопасности.

При внесении изменений учитываются:

1. результаты аудита информационной безопасности, а также результаты предыдущих аудитов;
2. рекомендации независимых экспертов по информационной безопасности;
3. существенные угрозы и уязвимости информационной системы;
4. отчеты об инцидентах в области информационной безопасности;
5. рекомендации органов государственной власти.

Пересмотр Политики осуществляется специалистами, ответственным за ее разработку, внедрение и включает оценку возможности улучшения ее положений и процесса управления информационной безопасностью в соответствии с изменениями.

Настоящая Политика подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков информационной безопасности в Обществе, и должна актуализироваться по мере необходимости.

Пересмотренная политика информационной безопасности утверждается уполномоченными лицами.

2. Меры по обеспечению безопасности информации

Система обеспечения безопасности информационных ресурсов Общества, его ведомств и подведомственных организаций предусматривает комплекс организационных, технических, программных средств и мер по защите информации:

1. в процессе документооборота;
2. при работе сотрудников с конфиденциальными документами и сведениями, составляющие служебную информацию;
3. при обработке информации в автоматизированных системах;
4. при передаче данных по каналам связи.

К правовым мерам защиты относятся действующее законодательство РК в сфере информационной безопасности, нормативно-правовые акты, принятые в Общества, его ведомств и организациях, находящихся в ведении Общества, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее

получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

Реализация указанных мер препятствует тем самым неправомерному использованию информации и является сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с сотрудниками (пользователями ИС) и обслуживающим персоналом.

Организационные меры защиты – меры административного и процедурного характера, регламентирующие процессы функционирования систем обработки данных, использование их ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с ИС, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Физические меры защиты основаны на применении специализированных механических, электро- или электронно-механических устройств и сооружений, предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам ИС и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов ИС (пломбы, наклейки и т.п.).

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в том числе в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

2.1. Защита общедоступной информации

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 Общества, 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.

2.2. Защита от ввода ошибочных данных

Данные, вводимые в приложениях, должны проверяться программными и техническими средствами, чтобы гарантировать их правильность и соответствующее использование. Ввод информации должен осуществляется лицами, функционально ответственными за данный вид работ и ознакомленными с соответствующими инструкциями.

2.3. Защита от неправомерной модификации передаваемых данных, технической и служебной информации

Кроме средств санкционированного доступа к коммуникационным средствам и сетевому оборудованию, защита передаваемых данных от модификации должна осуществляться программно-техническими и организационными мерами.

2.4. Защита системы архивирования

Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в помещении за пределами здания, где расположено основное серверное оборудование. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

2.5. Защита оборудования, оставленного без присмотра

Пользователи должны быть осведомлены о правилах безопасности и методах защиты оставленного без присмотра оборудования, а также об ответственности за ненадлежащее их исполнение.

В целях снижения рисков неавторизованного доступа, потери или повреждения информации следует применять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации.

Необходимо по возможности учитывать следующие мероприятия:

1. носители с важной или критичной служебной информацией, когда они не требуются или пустует помещение, следует убирать и запирать (например, в несгораемом сейфе или шкафу);

2. персональные компьютеры, компьютерные терминалы и принтеры должны быть выключены по окончании работы; следует также применять пароли или другие мероприятия в отношении устройств, находящихся без присмотра;

3. применить политику автоматического блокирования «рабочего стола» по истечению определенного времени;

4. необходимо обеспечить защиту пунктов отправки/приема корреспонденции, а также факсимильных и телексных аппаратов в случаях нахождения их без присмотра;

5. в нерабочее время фотокопировальные устройства следует защищать от неавторизованного использования;

6. напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно;

7. по решению руководства определенным сотрудникам на системном уровне ограничить авторизацию на ПК вне рабочего времени.

2.6. Управление доступом

Доступ к информационным ресурсам и системам Общества должны быть контролируемым с учетом требований деятельности организации и безопасности.

В Обществе, его ведомствах и организациях, находящихся в ведении Общества определены процедуры регистрации и снятия с регистрации пользователей в отношении предоставления доступа к информационным ресурсам и системам.

Предоставление и использование привилегированных разрешений ограничено и подлежит контролю во избежание сбоев систем по причине их возможного нецелесообразного использования.

Привилегии предоставляются сотрудникам только в случае производственной необходимости и только на время выполнения соответствующих авторизованных действий.

Обеспечивается процесс авторизации и регистрации всех предоставленных привилегий. Привилегии не предоставляются до завершения процесса авторизации.

Неотъемлемой составляющей системы управления доступом является организация парольной защиты доступа к информационным ресурсам и

системам Общества, его ведомств и организации, находящихся в ведении Общества.

Процедура регистрации организована таким образом, чтобы свести к минимуму возможность неавторизованного доступа.

Также ограничено и подлежит строгому контролю использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений.

Права доступа пользователей подлежат регулярному пересмотру для поддержания эффективного контроля доступа к данным информационным услугам.

2.7. Управление инцидентами информационной безопасности

Процедуры по мониторингу, оценке и управлению инцидентами информационной безопасности подлежат непрерывному усовершенствованию.

Необходимо обеспечить оперативность оповещения всеми пользователями ИС Общества, его ведомств и организации, находящихся в ведении Общества о событиях информационной безопасности и нарушениях информационной безопасности для своевременного реагирования и их устранения сотрудниками службы технической поддержки.

Установлены ответственность руководства и процедуры, гарантирующие быстрое и эффективное реагирование на инциденты.

Цели в области управления инцидентами информационной безопасности должны быть согласованы с руководством и сотрудниками, ответственными за управление инцидентами информационной безопасности.

Определяются механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям.

Необходимо фиксировать каждый инцидент с подробным описанием, информация должна быть собрана, сохранена и представлена на случай, если инцидент информационной безопасности может привести к судебному разбирательству.

2.8. Защита окружающей среды

Защита окружающей среды в Обществе, его ведомствах и подведомственных организациях характеризуется комплексом принятых мер, которые направлены на предупреждение отрицательного воздействия человеческой деятельности на окружающую природу, что обеспечивает благоприятные и безопасные условия человеческой жизнедеятельности.

В Обществе, его ведомствах и подведомственных организациях должны быть организованы меры по безопасной утилизации продуктов жизнедеятельности (макулатура, лампы освещения, бытовые химические вещества и пр.). Так же должны быть предусмотрены меры по утилизации Средства вычислительной техники (далее - СВТ) и носителей информации. Все действия по утилизации СВТ и носителей информации должны документироваться

3. 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 Общества, 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. 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:

1. 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;

2. мониторинг нарушения администраторами и пользователями информационных систем Общества 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:

1. контроля за реализацией требований политики информационной безопасности информационных систем Общества;
2. контроля за реализацией положений государственных нормативных актов по обеспечению информационной безопасности в информационных системах Общества;
3. выявления нештатных (или злоумышленных) действий в информационных системах Общества;
4. выявления потенциальных нарушений информационной безопасности;
5. 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.

4. Дополнительные требования

4.1. Обучение и повышение уровня знаний в области информационной безопасности

Необходимо проводить периодическое обучение и повышение квалификации сотрудников Общества 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.