Приложение 3
к постановлению правления
райпо
10.06.2024 № 119

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ЛУНИНЕЦКОГО РАЙПО

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика является документом, доступным любому работнику Лунинецкого райпо и пользователю его ресурсов, и представляет собой официально принятую правлением Лунинецкого райпо систему взглядов на проблему обеспечения информационной безопасности (далее - ИБ).

Правление Лунинецкого райпо осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в связи с изменением законодательства, регулирующего сферу электросвязи, реализуемыми технологиями, ожиданиями абонентов и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит Лунинецкому райпо обеспечить ее финансовую и экономическую стабильность, рентабельность и повышение имиджа.

Требования информационной безопасности, которые предъявляются Лунинецким райпо, соответствуют интересам (целям) деятельности организации и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

Настоящая Политика информационной безопасности Лунинецкого райпо (далее - Политика ИБ) разработана в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 № 64).

Термины и определения, используемые в настоящей Политике ИБ, понимаются в значениях, определенных для них Законом Республики Беларусь от 10.11.2008 №455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации», Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом Оперативно--аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 №64) и технических нормативных правовых актов Республики Беларусь (далее - ТНПА), регламентирующими

вопросы информационной безопасности (далее - ИБ).

Политика ИБ - это совокупность документированных правил, процедур и требований в области защиты информации, действующих в организации и содержащих:

цели создания системы защиты информации;

права и обязанности субъектов информационной системы (далее - ИС); порядок взаимодействия с иными информационными системами; перечень средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств технической защиты информации (далее - объекты ИС) и субъектов ИС, сведения о месте их размещения и порядке информационного взаимодействия субъектов ИС с объектами этой системы и объектов между собой;

способы разграничения доступа субъектов к объектам ИС; перечень организационных мер, направленных на реализацию требований по созданию системы защиты информации (далее - СЗИ);

порядок действий при возникновении угроз обеспечения конфиденциальности, целостности, доступности, подлинности и сохранности информации, в том числе чрезвычайных и непредотвратимых обстоятельств (непреодолимой силы), и при ликвидации их последствий; порядок резервирования и уничтожения информации; порядок защиты от вредоносного программного обеспечения; порядок выявления угроз, которые могут привести к сбоям, нарушению функционирования информационной системы;

порядок осуществления контроля (мониторинга) за функционированием ИС.

Настоящая Политика ИБ распространяется на все бизнес-процессы организации и обязательна для применения всеми работниками и руководством организации, а также пользователями его информационных ресурсов.

Общая структура Политики ИБ организации представляет собой многоуровневую иерархическую систему документов, имеющих различное назначение и область применения.

Политика ИБ организации - документ верхнего уровня, определяющий цели, содержание и основные направления деятельности организации по обеспечению ИБ.

Документы 2-го уровня - документы (стандарты, положения, регламенты), регулирующие деятельность по обеспечению ИБ в конкретных информационных системах или области деятельности, связанной с ИБ.

Документы 3-го уровня - документы (инструкции, технические требования и др.), детализирующие требования Политики ИБ применительно к одной или нескольким областям ИБ, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ, в рамках технологических процессов, используемых в организации, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, инструкции регламенты, порядки и др.).

Документы 4-го уровня - документы, содержащие результаты выполненной деятельности по обеспечению ИБ (формы, журналы, заявки, акты, протоколы и др.).

2.НОРМАТИВНАЯ ПРАВОВАЯ БАЗА СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основными нормативными правовыми документами, устанавливающими требования в сфере ИБ, а также являющимися основой для разработки настоящей Политики ИБ являются:

Закон Республики Беларусь от 10.11.2008 № 455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации».

Закон является комплексным нормативным правовым актом, направленным на регулирование общественных отношений, возникающих при: поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

организации и обеспечении защиты информации.

Положение о технической и криптографической защите информации в Республике Беларусь, утверждено Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», которое определяет правовые и организационные основы технической и криптографической защиты информации в Республике Беларусь.

Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденное приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 № 64), которое определяет:

комплекс мероприятий по защите информации, подлежащей обработке в информационной системе;

перечень требований к системе защиты информации, подлежащих включению в задание по безопасности на информационную систему или в техническое задание на информационную систему;

требования к Политике информационной безопасности;

требования по разработке локальных нормативных правовых актов организации в области защиты информации.

Положение о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации, утвержденное

приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 № 64), которое определяет:

требования к комплексу средств обеспечения безопасности средств криптографической защиты информации (далее - СКЗИ);

требования к обеспечению выполнения организационных и технических мер при применении СКЗИ для защиты служебной информации ограниченного распространения, определенной в соответствии с законодательством.

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденное приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь 11.10.2017 № 64).

3.ОПРЕДЕЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ЕЕ ОБЩИХ ЦЕЛЕЙ И ОБЛАСТИ ПРИМЕНЕНИЯ

ИБ представляет собой состояние защищенности информационных баз данных и поддерживающей инфраструктуры Лунинецкого райпо на всех этапах процессов создания, обработки, передачи и хранения информации от случайных или преднамеренных воздействий естественного или искусственного характера с целью недопущения нанесения ущерба деятельности организации.

Основными объектами защиты системы информационной безопасности в Лунинецком райпо являются:

информационные ресурсы, содержащие информацию, распространение и (или) предоставление которой ограничено в соответствии с законодательством Республики Беларусь, независимо от формы и вида ее представления;

информационные ресурсы, содержащие конфиденциальную информацию, а также внутреннюю информацию, необходимую для работы организации, независимо от формы и вида ее представления;

работники организации, являющиеся пользователями информационных систем райпо;

информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Требования по обеспечению информационной безопасности Лунинецкого райпо должны неукоснительно соблюдаться всеми работниками организации и другими сторонами, как это определяется локальными нормативными актами организации в области информационной безопасности, а также требованиями договоров и соглашений, участником, которых является организация.

Руководство организации приветствует и поощряет в установленном порядке деятельность работников организации и пользователей ее информационных систем по обеспечению ИБ Лунинецкого райпо.

Неисполнение или некачественное исполнение работниками Лунинецкого райпо и пользователями ее информационных систем обязанностей по обеспечению ИБ может повлечь лишение доступа к информационным системам, а также применение к виновным лицам и организациям правовых мер воздействия, степень которых определяется установленным в организации порядком и требованиями действующего законодательства Республики Беларусь.

Обеспечение ИБ - это непрерывный процесс, заключающийся в непрерывном управлении, контроле, выявлении слабых мест и потенциально возможных угроз, реализации наиболее рациональных и обоснованных форм и методов создания и совершенствования системы безопасности.

Обеспечение ИБ Лунинецкого райпо осуществляется на четырех уровнях:

законодательный уровень (законы, нормативные правовые акты, технические нормативные правовые акты);

административный уровень (действия общего характера, определенные локальными нормативными актами организации);

процедурный уровень (конкретные меры безопасности, обеспечиваемые сотрудниками);

технический уровень (конкретные технические меры).

Целями ИБ организации являются обеспечение сохранности и конфиденциальности информации, защита и гарантия доступности, достоверности и целостности информации, избежание утечки информации, минимизация ущерба от событий, несущих угрозу ИБ.

4.ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках реализации политики ИБ должны быть решены следующие задачи:

назначены и распределены роли в системе обеспечения ИБ;

определены объекты, подлежащие защите;

определены и прокатегорированы информационные активы, подлежащие защите;

определена ценность защищаемых активов и степень тяжести последствий от потери свойств ИБ для информационных активов;

обеспечена конфиденциальность информации в соответствии с проведенным категорированием информационных активов и ресурсов;

обеспечена целостность и учет информации на всех этапах, связанных с нею процессов (создание, обработка, хранение, передача и уничтожение);

обеспечена своевременная доступность информации авторизованным пользователям;

определены и актуализированы списки возможных негативных воздействий (угроз) на защищаемые активы, способов и степени вероятности реализации этих угроз (уязвимости);

обеспечена ИБ на всех этапах бизнес-процессов организации;

обеспечена наблюдаемость, направленная на фиксирование любой деятельности пользователей и процессов;

обеспечена защита от несанкционированного доступа и нерегламентированных действий в рамках представленных полномочий управления доступом и регистрацией всех действий в ИС организации, оборудовании и т.д.;

обеспечена антивирусная защита;

регламентировано использование ресурсов сети Интернет;

регламентировано использование СКЗИ;

обеспечена защита технологических процессов организации; обеспечен необходимый уровень отказоустойчивости ИТ-сервисов и доступности данных для управлений, отделов, секторов (далее-подразделений) организации, достигаемый через внедрение постоянно обновляемых планов обеспечения непрерывной работы и восстановления работоспособности, как в целом организации, так и отдельных подразделений, и с помощью других процедур (резервное копирование, кластеризация, резервирование).

При обеспечении ИБ Лунинецкого райпо должны соблюдаться следующие принципы:

принцип равноправности - означает обеспечение защиты оборудования, программного обеспечения и систем управления от всех видов угроз;

принцип непрерывности - предусматривает непрерывное обеспечение безопасности информационных ресурсов и ИС организации;

принцип рациональности - стоимость затрат на средства защиты, не должны превышать размера убытков, которые могут возникнуть в случае нарушения ИБ;

принцип комплексности - для обеспечения безопасности во всем многообразии структурных элементов, угроз и каналов несанкционированного доступа должны применяться все виды и формы защиты в полном объеме. Недопустимо применять отдельные формы или технические средства;

принцип комплексной проверки - заключается в осуществлении контроля, проведения проверок и анализа оборудования, контроля программных средств. Должен осуществляться непрерывный мониторинг аварийных сообщений и параметров ошибок, постоянно должно выполняться контроль работоспособности аппаратного и программного оборудования, а также контроль целостности программных средств, как при загрузке, так и в процессе их функционирования;

принцип надежности - методы, средства и формы защиты должны надежно перекрывать все пути проникновения и возможные каналы утечки информации, для этого допускается дублирование средств и мер безопасности;

принцип универсальности - меры безопасности должны перекрывать пути угроз независимо от места их возможного воздействия;

принцип централизованного управления - в рамках определенной структуры должна обеспечиваться организованно-функциональная самостоятельность процесса обеспечения ИБ;

принцип целенаправленности - необходимо защищать то, что должно защищаться в интересах конкретной цели;

принцип квалификации обслуживающего персонала - обслуживание оборудования должно осуществляться сотрудниками, подготовленными не только в вопросах эксплуатации техники и ПО, но и в технических вопросах обеспечения безопасности информации;

принцип ответственности - границы ответственности за обеспечение ИБ должны быть четко установлены, полномочия по обеспечению ИБ строго распределены.

5.НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОБЩИЕ РОЛИ, СВЯЗАННЫЕ С ОБЕСПЕЧЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные направления деятельности Лунинецкого райпо в сфере обеспечения ИБ заключаются в:

реализации комплекса организационных мероприятий по управлению ИБ, а также реализации комплекса аппаратных, программно-аппаратных, программных и технических средств защиты информации при ее автоматизированной обработке, хранении и передаче по каналам связи;

обеспечении бесперебойности работы организации и защиты важных активов ИС от последствий существенных сбоев или отказов, а также обеспечение их своевременного восстановления;

проведении мероприятий по обеспечению ИБ в ИС в соответствии с действующими нормативными правовыми актами и техническими нормативными правовыми актами Республики Беларусь в области защиты информации, а также локальными нормативными актами организации.

Ответственность за организацию и контроль работ по защите информации в Лунинецком райпо возлагается на ведущего специалиста по сопровождению программного обеспечения райпо.

К работам по созданию системы защиты информации ИС райпо могут дополнительно привлекаться организации, имеющие соответствующие специальные разрешения (лицензии) Оперативно аналитического центра при Президенте Республики Беларусь.

Главная цель создания СЗИ - достижение максимальной эффективности защиты за счет одновременного использования всех необходимых ресурсов, методов и средств, исключающих несанкционированный доступ к защищаемой информации и обеспечивающих физическую сохранность ее носителей.

6.УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все множество потенциальных угроз ИБ делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с возможной противоречивостью требований регуляторов и контрольных органов, с действиями менеджмента организации, неадекватными целям и сложившимся условиям, с человеческим фактором, касающимся работников организации, работников подведомственных организаций, посторонних лиц.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре организации могут быть как внешними, так и внутренними.

7.МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

По отношению к организации нарушители могут быть разделены на внешних и внутренних нарушителей.

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей организации рассматриваются:

работники организации - зарегистрированные пользователи информационных систем (которые имеют логин, пароль и доступ к корпоративной сети); работники организации, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам

информационных систем организации, но имеющие доступ в здания и помещения;

персонал, обслуживающий технические и программные средства информационных систем организации;

работники структурных подразделений организаций, привлеченных организаций, задействованных в разработке и (или) технической поддержке программного обеспечения;

руководители различных уровней.

Внешние нарушители.

В качестве потенциальных внешних нарушителей организации рассматриваются:

бывшие работники организации;

представители подрядных организаций;

посетители зданий и помещений организации;

представители конкурирующих с организацией структур, работающих в аналогичных сферах деятельности;

члены преступных групп и организаций;

лица, случайно или умышленно проникшие в информационные системы организации из внешних телекоммуникационных сетей;

другие, посторонние лица, получившие неправомерный доступ к конфиденциальной и другой защищаемой информации организации.

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

нарушитель скрывает свои несанкционированные действия от других работников организации;

несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

внешний нарушитель может действовать в сговоре с внутренним нарушителем.

8. УПРАВЛЕНИЕ ПОЛИТИКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Совокупность документированных правил, процедур и требований в области защиты информации, являющихся составной частью Политики ИБ, закрепляется Положением о системе управления информационной безопасностью Лунинецкого райпо, разрабатываемым организацией.

В рамках управления Политикой ИБ в Положении о системе управления информационной безопасностью Лунинецкого райпо закрепляются нормы,

обязательные для ознакомления и выполнения всеми работниками райпо, а также лицами, работающими с принадлежащими организации информацией и информационными ресурсами в рамках заключенных с ней договоров и соглашений, в целях обеспечения ИБ, управления непрерывностью деятельности райпо, ликвидации последствий нарушений политики ИБ, определения общих и специальных обязанностей работников по управлению ИБ, включая отчеты об инцидентах безопасности, а также правила безопасности, которым должны следовать работники и др.

9. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изменение норм, содержащихся в настоящей Политике, производится в следующих случаях:

изменения требований законодательства Республики Беларусь, нормативных правовых и технических нормативных правовых актов, методических документов Министерства связи и информатизации Республики Беларусь, Оперативно-аналитического центра при Президенте Республики Беларусь, других органов управления, регулирующих сферу ИБ;

необходимостью регламентации (детализации) процедур в рамках Политики ИБ, по результатам практики ее применения, возникновения нестандартных ситуаций, угроз и иных факторов, способных оказать прямое влияние на ИБ Лунинецкого райпо, оценки влияния на компанию внешних и внутренних факторов, результатам оценки рисков, результатов проверки Политики информационной безопасности.

Настоящая Политика ИБ, все изменения и дополнения к ней утверждаются постановлением правления Лунинецкого райпо и является обязательной к ознакомлению и соблюдению (или исполнению) всеми участниками (пользователями) информационной системы Лунинецкого райпо.