КАЛУГАИНФОРМТЕХ

Государственное бюджетное учреждение
Калужской области
«Агентство информационных технологий
Калужской области»

(ГБУ КО «Калугаинформтех»)

П Р И К А З

от «20» октября 2023 г. **№ 37**

Об утверждении политики
информационной безопасности
ГБУ КО «Калугаинформтех»

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и нормами действующего законодательства **ПРИКАЗЫВАЮ:**

1. Утвердить Политику информационной безопасности ГБУ КО «Калугаинформтех» (Приложение).
2. Приказ ГБУ КО «Калугаинформтех» от 01.03.2021 № 16 признать утратившими силу.
3. Главному специалисту отдела ОПиКО Альминайте Я.С. ознакомить заинтересованных сотрудников учреждения с настоящим приказом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **А.С. Корабанов**

ПРИЛОЖЕНИЕ
к приказу
ГБУ КО «Калугаинформтех»
от 20 октября 2023 г. № 37

Политика информационной безопасности государственного бюджетного учреждения Калужской области «Агентство информационных технологий Калужской области»

1. Общие положения

1.1. Введение

Политика информационной безопасности ГБУ КО «Калугаинформтех» (далее – Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

1.2. Цели

Основными целями политики ИБ являются защита информации Учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ осуществляет директор Учреждения. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет директор Учреждения.

Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Задачи

Политика информационной безопасности (далее – ПИБ) направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи, хранении информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба Учреждению обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Разработанная на основе прогноза ПИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Учреждения. Необходимо

учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации системы управления ИБ в Учреждении;
- определение ПИБ.

1.4. Область действия

ПИБ распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками и должностными лицами.

Положения ПИБ применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.5. Период действия и порядок внесения изменений

Настоящая политика вводится в действие приказом директора Учреждения.

Политика признается утратившей силу на основании приказа директора Учреждения.

Изменения в политику вносятся приказом директора Учреждения.

Инициаторами внесения изменений в ПИБ являются:

- директор Учреждения
- заместитель директора, курирующий данное направление.

Плановая актуализация ПИБ производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Учреждения;
- при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб Учреждения.

2. Политика информационной безопасности Учреждения

2.1. Назначение политики информационной безопасности

Политика информационной безопасности Учреждения (ПИБ) – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Учреждении.

Под ПИБ понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

ПИБ относятся к административным мерам обеспечения ИБ и определяют стратегию Учреждения в области ИБ.

ПИБ регламентирует эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя

поведение информационной системы (дале – ИС) и ее пользователей в различных ситуациях.

ПИБ реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие ПИБ, должны быть утверждены директором Учреждения.

2.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ следующие:

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

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ Учреждения, корректировка моделей угроз;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Учреждения, а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности, в рамках исполнения должностных обязанностей.

2.3. Соответствие политики информационной безопасности действующему законодательству

Правовую основу ПИБ составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственной власти различного уровня в пределах их компетенции.

2.4. Ответственность за политику информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт директор Учреждения.

Ответственность за реализацию ПИБ возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты, а также доведения правил ПИБ до сотрудников Учреждения – на заместителя директора, курирующего данное направление;

– в части, касающейся исполнения правил ПИБ, – на каждого сотрудника Учреждения, в рамках их должностных и функциональных обязанностей, и иных лиц, попадающих под область действия настоящей ПИБ.

2.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Учреждения в области ИБ возлагается на сотрудник, в должностные обязанности которого входят вопросы по информационной безопасности учреждения. Обучение сотрудников Учреждения правилам обращения с конфиденциальной информацией проводится путем:

– проведения инструктивных занятий с сотрудниками;

– самостоятельного изучения сотрудниками внутренних нормативных документов Учреждения, а также норм действующего законодательства в области защиты информации.

Допуск персонала к работе с конфиденциальной информацией и защищаемыми информационными ресурсами Учреждения осуществляется только после его ознакомления с ПИБ, а также иными инструкциями пользователей отдельных информационных систем.

Правила допуска к работе с конфиденциальной информацией и защищаемыми информационными ресурсами лиц, не являющихся сотрудниками Учреждения, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

2.6. Защищаемые информационные ресурсы Учреждения

Различаются следующие категории информационных ресурсов, подлежащих защите в Учреждении:

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным Законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», Постановлением правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах.

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности Учреждения, которую запрещено относить к конфиденциальной на основании законодательства Российской Федерации. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Учреждения;

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, включая персональные данные, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются локальными актами учреждения.

Подходы к решению проблемы защиты информации в Учреждении, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Учреждения.

Для этого в Учреждении выполняются следующие мероприятия:

– определяется порядок работы с документами, содержащими конфиденциальные сведения;

– устанавливается круг лиц и порядок доступа к подобной информации;

– вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;

– включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма обязательства о неразглашении сведений конфиденциального характера подписывается при заключении трудового договора, который подписывается всеми сотрудниками Учреждения при приеме на работу. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Учреждением с другими организациями.

Согласно пункта 7 статьи 86 Трудового кодекса Российской Федерации защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

При передаче персональных данных сотрудника работодатель должен соблюдать требования статьи 88 Трудового кодекса Российской Федерации.

Согласно статье 90 Трудового кодекса Российской Федерации лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, материальную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

2.6.1. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений ПИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Учреждении и проведение разъяснительной работы по ИБ среди сотрудников.

Сотрудник, в должностные обязанности которого входят вопросы по информационной безопасности учреждения собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения Учреждения. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Сотрудник, в должностные обязанности которого входят вопросы по информационной безопасности учреждения организовывает периодическую проверку ресурсов Учреждения путем моделирования возможных попыток осуществления несанкционированного доступа к защищаемым информационным ресурсам.

Плановая разъяснительная работа по правилам ПИБ, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Учреждении, проводится ежеквартально.

Внеплановая разъяснительная работа по правилам настоящий политики, а также инструктаж сотрудников Учреждения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в Учреждении, проводится при пересмотре ПИБ, при возникновении инцидента нарушения правил ПИБ.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями ПИБ.

2.6.2. Ликвидация последствий нарушения политики информационной безопасности

Сотрудник, в должностные обязанности которого входят вопросы по информационной безопасности учреждения, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления несанкционированного доступа к защищаемым информационным ресурсам ИС рекомендуется уведомить сотрудника, в должностные обязанности которого входят вопросы по информационной безопасности учреждения или руководство Учреждения и далее следовать их указаниям.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

2.6.3. Ответственность нарушителей политики информационной безопасности

Ответственность за нарушение правил ПИБ несет каждый сотрудник Учреждения в рамках своих должностных обязанностей и полномочий.

На основании статьи 192 Трудового кодекса РФ сотрудники, нарушающие требования ПИБ Учреждения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил ПИБ (статья 238 Трудового кодекса Российской Федерации).

3. Регулирующие законодательные документы

При организации и обеспечении работ по ИБ сотрудники Учреждения должны руководствоваться следующими законодательными нормативными документами:

3.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

– Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении доктрины информационной безопасности Российской Федерации»).

3.2. Законы Российской Федерации

– Уголовный кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Федеральный закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3.3. Указы и распоряжения президента Российской Федерации

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

3.4. Постановления и распоряжения правительства Российской Федерации

– Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»;

– Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

– Постановлением правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».