УТВЕРЖДЕНА
приказом Министерства социальной защиты Алтайского края
от 31.03.2022 № 27/Пр/119

ПОЛИТИКА
информационной безопасности Министерства социальной защиты Алтайского края

1. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.
АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
ИБ – Информационная безопасность.
ИР – Информационные ресурсы.
ИС – Информационная система.
КИ — Конфиденциальная информация.
МЭ – Межсетевой экран.
ЛВС — Локальная вычислительная сеть.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПДн – Персональные данные.
ПО – Программное обеспечение.
СЗИ – Средство защиты информации.
СУИБ – Система управления информационной безопасностью.
ЭВМ – Электронная – вычислительная машина, персональный компьютер.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет

ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между ЛВС и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых для обеспечения информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организа-

ции (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети.

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Основные сведения

Политика ИБ Министерства социальной защиты Алтайского края(далее – Оператор) определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Оператор в своей деятельности.

Основными целями Политики ИБ являются защита информации Оператора от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении о деятельности Оператора.

Общее руководство обеспечением ИБ осуществляется руководителем Оператора. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ответственный сотрудник, определенный руководителем Оператора. Ответственность за функционирование информационных систем Оператора несет администратор ИС.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

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

Сотрудники Оператора обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов Оператора по вопросам обеспечения ИБ.

Политика ИБ 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 и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба Оператору обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Оператора), либо иметь непреднамеренный ошибочный характер.

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ у Оператора на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза Политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Оператора. 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 СУИБ;

определение порядка сопровождения ИС Оператора.

Настоящая Политика распространяется на все структурные подразделения Оператора и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

Настоящая Политика вводится в действие приказом руководителя Оператора.

Политика признается утратившей силу на основании Приказа руководителя Оператора.

Политику ИБ определяет:

Политика реализации антивирусной защиты;

Политика учетных записей; политика предоставления доступа к ИР;

Политика использования паролей; политика защиты АРМ;

Политика конфиденциального делопроизводства.

3. Область действия. Период действия и порядок внесения изменений

Изменения в Политику вносятся приказом руководителя Оператора. Инициаторами внесения изменений в Политику информационной безопасности являются:

руководитель Оператора;

руководители подразделений Оператора;

администратор информационной безопасности.

Плановая актуализация настоящей Политики 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 внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Оператора;

при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб Оператору.

Ответственными за актуализацию Политики ИБ (плановую и внеплановую) является АИБ.

Контроль за исполнением требований настоящей Политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

4. Политика информационной безопасности. Назначение Политики инфор-

мационной безопасности. Основные принципы обеспечения информационной безопасности

Политика ИБ Оператора – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации у Оператора.

Политика ИБ относится к административным мерам обеспечения ИБ и определяет стратегию Оператора в области ИБ.

Политика ИБ регламентирует эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика ИБ реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, должны быть утверждены руководителем Оператора.

Основными принципами обеспечения ИБ являются следующие:

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

своевременное обнаружение проблем, потенциально способных повлиять на ИБ Оператора, корректировка моделей угроз и нарушителя;

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 Оператора, а также повышать трудоемкость технологических процессов обработки информации;

контроль эффективности принимаемых защитных мер;

персонификация и адекватное разделение ролей и ответственности между сотрудниками Оператора, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. Соответствие Политики информационной безопасности действующему законодательству

Правовую основу Политики 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 государственного управления различного уровня в пределах их компетенции.

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию Политики возлагается:

в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

в части, касающейся доведения правил Политики до сотрудников Оператора, а также иных лиц (область действия настоящей Политики) – на АИБа;

в части, касающейся исполнения правил Политики, – на каждого сотрудника Оператора, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

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

Организация обучения сотрудников Оператора в области ИБ возлагается на АИБа. Обучение проводится согласно утвержденному Плану.

Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Допуск персонала к работе с защищаемыми ИР Оператора осуществляется только после его ознакомления с настоящей Политикой, а также после ознакомления пользователей с «Порядком работы пользователей в информационных системах», а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в журналах ознакомления.

Допуск персонала к работе с КИ Оператора осуществляется после ознакомления с «Порядком организации работы с материальными носителями конфиденциальной информации», «Порядком организации работы с электронными и машинными носителями конфиденциальной информации». Правила допуска к работе с ИР лиц, не являющихся сотрудниками Оператора, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

7. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР Оператора.

Положения данной Политики определены в «Положении о разрешительной системе допуска к информационным системам персональных данных», утверждаемом соответствующим приказом руководителя Оператора.

8. Политика учетных записей

Настоящая Политика определяет основные правила присвоения учетных записей пользователям информационных активов Оператора.

Регистрационные учетные записи подразделяются на:

пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Оператора;

административные – предназначенные для администрирования информационных активов;

системные – используемые для нужд операционной системы;

служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Оператора назнача-

ется уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

9. Политика использования паролей

Настоящая Политика определяет основные правила парольной защиты у Оператора.

Положения Политики закрепляются в «Порядке организации парольной защиты в информационных системах».

10. Политика реализации антивирусной защиты

Настоящая Политика определяет основные правила для реализации антивирусной защиты у Оператора.

Положения Политики закрепляются в «Порядке проведения антивирусного контроля в информационных системах».

11. Политика защиты автоматизированного рабочего места

Настоящая Политика определяет основные правила и требования по защите информации Оператора от неавторизованного доступа, утраты или модификации.

Положения данной Политики определяются в соответствии с используемым техническим решением.

12. Профилактика нарушений Политик информационной безопасности

Под профилактикой нарушений Политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ у Оператора и проведение разъяснительной работы по ИБ среди

пользователей.

13. Ликвидация последствий нарушения Политик информационной безопасности

Администратор сети, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать их указаниям.

Действия АИБа и администратора ИС при признаках нарушения Политик информационной безопасности регламентируются следующими внутренними документами:

Политикой информационной безопасности;

Порядок работы пользователей в ИС;

Регламент администратора ИС.

14. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник Оператора в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ Оператора, 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 Оператору в результате нарушения ими правил Политики ИБ (ст. 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Оператора несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.